Online Safety Policy

This policy applies to the whole school including Boarding and the Early Years. The current version of any policy, procedure, protocol or guideline is the version held on the TASIS England website. It is the responsibility of all staff to ensure that they are following the current version.

Information Sharing Category	PUBLIC
TASIS England Document reference (Org, Doc, version, date)	TASIS_OnlineSafety_V10.4_01092026
Version	10.4
Date published	01 September 2026
Date ratified by Head of School	01 September 2026
Review/Update date	01 September 2027
Responsible area	Designated Safeguarding Lead & Head's Office

Agreed by:

Head of School	**Chair of the Board**
Bryan Nixon	David King
01 September 2026	01 September 2026

Introduction: The purpose of this policy is to safeguard all individuals at TASIS England—including students, faculty, staff, contractors, consultants, volunteers, bank and agency workers—by maintaining a safe electronic environment. (**the terms 'faculty' and 'staff' are used interchangeably within this policy and any reference to faculty or staff refers to any person employed at TASIS England whether they are directly employed, contractors, consultants, volunteers, bank or agency**). This policy is publicly available on the school website. All members of the TASIS community, including those who work, volunteer, or provide services to our school, share equal responsibility in understanding and implementing this policy and its procedures both during and outside of school hours, including activities away from school premises.

This policy aligns with current legislative requirements and integrates best practices drawn from a range of authoritative sources. The policy details the specific actions and behaviours required to achieve this and underscores the school's whole-school approach to Online Safety, which is seamlessly integrated into our broader safeguarding strategy.

Our key message is to ensure the safety of students and young people, a message that is applied to both online and offline behaviours. Online safety at TASIS England is a running and interrelated theme across all school policies and procedures. These connections ensure that Online Safety considerations are reflected in every aspect of our school's operations—from curriculum development and staff training to parental engagement and community involvement.

The faculty, staff, and student Acceptable Use Policies (AUP) are central to our Online Safety Policy and should be consulted alongside this policy. Moreover, the Online Safety Policy plays a critical role in our Safeguarding Children and Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. Given that a significant portion of radicalization cases occur through online mediums, our faculty and staff are trained to be vigilant and responsive to such risks, following the prescribed reporting procedures outlined in our safeguarding policies.

For the purposes of this document, the term "Board of Directors" is deemed to have the same meaning as "Proprietor" in accordance with the Independent Schools Standards Regulations (ISSR) and is used interchangeably. The governing bodies and proprietors ensure that Online Safety remains a consistent and interrelated theme while devising and implementing the whole school approach to safeguarding. This includes ensuring that Online Safety considerations are reflected in all relevant policies, curriculum planning, teacher training, and parental engagement strategies. The terms "faculty" and "staff" may be used interchangeably and refers to any person engaged or employed by the school to provide services and includes all TASIS England employees, directors, contractors, work experience / placement students, bank or agency staff and volunteers. Additionally, the terms "students" and "children" may be used interchangeably in this policy, with both terms referring to all those under or over the age of 18 years enrolled at TASIS England.

Monitoring and Review: This policy is subject to continuous monitoring, refinement and audit by The Head of School and the Designated Safeguarding Lead (DSL). The DSL and the Board of Directors will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged, with input from the Student Council regarding any updates to the Student Acceptable Use Policy (AUP). This discussion will be formally documented in writing. The Board of Directors recognises that staff builds expertise by undertaking safeguarding training and managing safeguarding concerns. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff

will be informed of the update/reviewed policy, and it is made available to them in either a hard copy or electronically.

Annual Governance Reporting: Each academic year the Board receives a written report covering Online Safety, filtering and monitoring, and cyber security. The report summarises incidents and trends, any changes to systems, training delivered, outcomes of tests/exercises, and planned improvements. Actions arising are tracked to completion.

Roles and Responsibilities: Our Designated Safeguarding Lead (Whole School) (working in conjunction with our IT Manager, Online Safety Coordinator and the Head of School) is responsible for ensuring the Online Safety of the school community. Our IT Manager will take operational responsibility for Online Safety, but the overall responsibility will fall on the DSL for making sure that policy is enforced and that the necessary checks, filters and monitoring are in place. They also have a specific duty of care to ensure that the schools' IT systems are secured and risk-assessed and based on school policies. Their role, in collaboration with the TASIS England IT Department, will include ensuring:

- Students know how to use the internet and connected devices responsibly and that parents and teachers have the knowledge and appropriate measures in place to keep students safe from exploitation or radicalisation.
- Students are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- To ensure that students use IT safely and securely and are aware of both external and peer to peer risks when using IT, including cyberbullying and other forms of abuse.
- Children, faculty, staff, the Board of Directors and volunteers will receive the appropriate Online Safety training, guidance, time and resources to effectively implement Online Safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal IT equipment by all individuals who affect or come into contact with the PreK-Grade 8 and US setting. Such policies and procedures are to include the personal use of work-related resources.
- The Acceptable Use Policy (AUP) is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be transparent and updated as agreed in school policies.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- An appropriate level of authorisation is to be given to IT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- A current record of all staff and students who are granted access to the school IT system is maintained.

Designated Safeguarding Lead (DSL): The Designated Safeguarding Lead (DSL) who is a member of the senior leadership team (SLT) has relevant, current and practical knowledge and understanding of safeguarding, child protection and Online Safety. Access to an individual holding this role is available at all times, for example, a Deputy Designated Safeguarding Lead is also in place should the DSL be absent. The designated persons for safeguarding will be responsible for ensuring:

- agreed policies and procedures are to be implemented in practice;
- all updates, issues and concerns are to be communicated to all IT users;
- the importance of Online Safety in relation to safeguarding is to be understood by all IT users;
- Updating and delivering staff training on Online Safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring;
- the training, learning and development requirements of staff are to be monitored and additional training needs identified and provided for boarding specific training;
- an appropriate level of access authorisation is given to IT users.

Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of students and young people will address Online Safety. A safe IT learning environment is to be promoted and maintained.

The Board of Director's responsibilities: Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the Board of Directors will do all that they reasonably can to limit children's exposure to risks when using the school's IT system. As part of this process, the Board of Directors has ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified.

All Staff: It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of TASIS England, and to deal with incidents of such a priority. All staff are responsible for ensuring they are up to date with current Online Safety issues, and this Online Safety Policy. Cyberbullying incidents will be reported in accordance with TASIS England's Anti-Bullying Policy. All staff will ensure they understand and adhere to our staff Acceptable Use Policy, which they must sign and return to the Online Safety Coordinator and a copy placed on faculty/staff file. Teachers will ensure they are confident in delivering the school's computing and Online Safety curriculum as required, identifying risks and reporting concerns as they arise.

Parents: Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. TASIS England will support parents with Online Safety guidance which is regularly shared through our website, newsletters, social media platforms and regular safety briefings via email, raising any concerns that they have.

All Students: All students will ensure they understand and adhere to our student Acceptable Use Policy, which they must sign and return to the Online Safety Coordinator. Students are reminded of their responsibilities regarding the use of the school's IT systems and equipment, including their expected behaviour.

Visitors and Members of the Community: Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use agreement.

Breadth of Online Safety Issues: We classify the issues within Online Safety into **four** areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users or with generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, images generated using AI ('deepfakes') and online bullying; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. Where members of the school community are felt to be at risk, this will be reported to the Anti-Phishing Working Group (https://apwg.org/).

These issues are to be managed by reducing availability, restricting access, and promoting safe and responsible use.

The following is a list of possible risks students may face in their access to technology:

- Access to illegal, harmful or inappropriate images or content
- The risk of being subject to grooming by those whom they contact on the internet
- Inappropriate and unsafe communication with strangers
- Cyberbullying
- Access to pornographic material
- Access to extremist material that could lead to radicalisation of students
- Access to unsuitable video or gaming sites
- Sites that encourage gambling
- Illegal downloading of material that breaks copyright laws
- Unauthorised access to/loss of/sharing of personal information

The above risks can be realised through a wide range of technologies, including:

- e-mail
- Smart phones, tablets and laptops, etc.
- The Internet (web)
- Social networking sites; X, YouTube, Facebook etc.
- Gaming sites
- Blogs, instant messaging, chat rooms, message boards, virtual learning environments
- Webcams, video hosting sites
- Photography

Faculty and Staff/Volunteers Use of IT Systems: Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the Faculty and Staff Code of Conduct pertaining to IT (please see appendices) before using any school IT resource. In addition:

- All faculty and staff including the Board of Directors will receive appropriate Online Safety training, which is updated regularly;
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password protected computers and other devices. Staff are advised to follow the "How do I stay secure on the Internet?" section in the Online Safety FAQ document.

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the students visit. Student internet usage is also monitored through the School's filtering and monitoring systems, which identify and manage access to blocked or inappropriate content in accordance with the School's safeguarding arrangements.
- Occasionally students may need to research educational material that may normally result in websites being blocked (e.g., racism). In this situation, staff may request to remove these sites from the filtered list for the period of study. Every request to do so should be auditable with clear reasons for the need.
- The Internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g., SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved web browsers and email systems which have appropriate security in place. Additionally, files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programs.
- Additionally, staff should not communicate with students through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used for this purpose.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e., videos of lessons, activities or fieldtrips, must be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.
- In order to strengthen the schools' defences against future cyber incidents, staff are expected to enable Multi-Factor Authentication (MFA) for all school online platforms.
- Network and device monitoring is undertaken for safeguarding and security purposes, is proportionate to risk, and is explained in staff and student AUPs and the school's privacy information.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

- Report in confidence to the Head of School (faculty/staff) or the DSL (students).
- The Head of School or DSL should investigate the incident accordingly.
- If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
- In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
- No student or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

Teaching About Online Safety: The school's Internet access is designed to enhance and extend education. Students will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use. Access levels reflect the curriculum requirements and age of students. Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity. Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of online materials is a part of teaching/learning in every subject.

Staff should be vigilant in lessons where students use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with school policy. Staff will be provided with sufficient Online Safety training to protect students and themselves from online risks and to deal appropriately with Online Safety

incidents when they occur. Ongoing staff development training includes training on Online Safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements.

Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help students to navigate the online world safely and confidently regardless of the device, platform or app. Online Safety is a focus in all areas of the curriculum and key Online Safety messages are reinforced regularly, teaching students about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Our Digital Citizenship and PSHEE Program is closely linked with our Relationships and Sex Education and PSHEE Programs and discusses the links associated with online abuse and other associated risks. Access levels to IT reflect the curriculum requirements and age of students. Faculty/staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity. Students will explicitly be taught the following topics through their lessons:

- What Internet use is acceptable and what is not and given clear guidelines for Internet use including protecting their online identity and privacy;
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications;
- How to evaluate what they see online;
- How to recognise techniques used for persuasion;
- Online behaviour;
- How to identify online risks
- How and when to seek support and report a range of concerns;
- How to recognise and respond to harmful online challenges and online hoaxes.

We recognise that Child-on-Child abuse can occur online and to this end we teach students how to spot early warning signs of potential abuse, and what to do if students are subject to sexual harassment online. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- access to illegal, harmful or inappropriate images;
- cyberbullying;
- access to, or loss of, personal information;
- access to unsuitable online videos or games;
- loss of personal images;
- inappropriate communication with others;
- illegal downloading of files;
- exposure to explicit or harmful content, e.g., involving radicalisation;
- plagiarism and copyright infringement; and
- sharing the personal information of others without the individual's consent or knowledge.

Online Safety education is reinforced throughout the year within and alongside our PSHEE program, these key messages and resources are shared with parents to discuss at home as well. We recognise a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, will be used. Staff should be vigilant in lessons where students use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with

school policy. Our curriculum and risk assessments address the Online Safety '4 Cs' (Content, Contact, Conduct, Commerce), including misinformation, disinformation (including fake news) and conspiracy theories. Students are taught to evaluate sources, recognise manipulation, and report concerns.

Harmful Online Challenges and Online Hoaxes: (Please refer to the latest DfE Guidance) There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach students to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern. Where a child or member of faculty/staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within Online Safety lessons, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

A case-by-case assessment, establishing the scale and nature of the possible risk to our students will be carried out, and appropriate actions taken, which may include sharing information with parents and carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw students' attention to a potential risk.

Our DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents and carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

Students Use of IT Systems: All students must agree to the IT Acceptable Use Policy before accessing the school systems. Students at TASIS England will be given supervised access to our computing facilities and will be provided with access to filtered Internet (see FAQ Document) and other services operating at the school (Student internet usage is monitored through the School's filtering and monitoring systems). The promotion of Online Safety within IT activities is to be considered essential for meeting the learning and development needs of students and young people. The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law. TASIS England will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's IT education and is also embedded in our Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- Education for a connected world
- The UK Safer Internet Centre (http://www.saferinternet.org.uk/)
- CEOP's Thinkuknow website (https://www.ceopeducation.co.uk/)
- Teaching Online Safety in School https://www.gov.uk/government/publications/teaching-online-safety-in-

schools

- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

Network and device monitoring is undertaken for safeguarding and security purposes, is proportionate to risk, and is explained in staff and student AUPs and the school's privacy information.

Educating Faculty/Staff: A planned calendar program of Online Safety training opportunities will be available to all staff members (including the Board of Directors, including whole charity activities and CPD training courses. Faculty/staff will be provided with sufficient Online Safety training to protect students and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development training includes training in Online Safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. Faculty/staff will undergo Online Safety training annually/when changes occur to ensure they are aware of current Online Safety issues and any changes to the provision of Online Safety, as well as current developments in social media and the internet as a whole. All faculty/staff will employ methods of good practice and act as role models for young people when using the internet and other digital devices. All faculty/staff will be educated on which sites are deemed appropriate and inappropriate. All faculty/staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism. Any new faculty/staff members are required to undergo Online Safety training as part of their induction program, ensuring they fully understand this Online Safety policy/social media policy/user agreement. The Online Safety Coordinator will act as the first point of contact for faculty/staff requiring Online Safety advice via regular TASIS Telegram articles on Online Safety.

Communicating and Educating Parents/Guardians in Online Safety: Parents will be provided with a copy of the IT User Acceptance Policy, and parents will be asked to sign it, as well as students aged eight and older. TASIS England recognises the crucial role that parents play in the protection of their children with regards to Online Safety. The school organises an annual awareness session for parents with regards to Online Safety which looks at emerging technologies and the latest ways to safeguard students from inappropriate content. The school will also provide parents and carers with information through newsletters, web sites and the parent portals. Parents and guardians are always welcome to discuss their concerns on Online Safety with the school, who can direct them to the support of our Online Safety Coordinator if required. Parents and carers will be encouraged to support the school in promoting good Online Safety practice.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), each as amended by the Data (Use and Access) Act 2025. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private as part of our Online Safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will act responsible for ensuring we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Radicalisation and the Use of Social Media to Encourage Extremism: The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme

ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people;
- Confirming extreme beliefs;
- Accessing likeminded people where they are not able to do this off-line, creating an online community;
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

TASIS England has a number of measures in place to help prevent the use of social media for this purpose:

- Web site filtering is in place on the school network to help prevent access to terrorist and extremist material and social networking sites such as TikTok, Snapchat, Facebook, Instagram, X by students.
- Students, parents and staff are educated in safe use of social media and the risks posed by online activity, including from extremist and terrorist groups.

Reporting of Online Safety Issues and Concerns Including Concerns Regarding Radicalisation: TASIS England has clear reporting mechanisms in place, available for all users to report issues and concerns. For faculty and staff any concerns regarding Online Safety should be made to the DSL who will work closely with the Online Safety Coordinator to review the issue and take the appropriate action. Students should raise any concerns with their class teacher who will then pass this on to the DSL and the Online Safety Coordinator. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children and Child Protection Policy. Our Designated Safeguarding Lead provides advice and support to other members of faculty/staff on protecting students from the risk of online radicalisation. TASIS England ensures faculty/staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify students at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Faculty/staff safeguard and promote the welfare of students and know where and how to refer students and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Emerging technologies, such as mobile phones with Internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- We carry out an annual audit of our Online Safety provision to establish if the Online Safety Policy is sufficiently robust and that the implementation of the Online Safety Policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Section Heads will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems apart from filtered *Wi-Fi* access.
- TASIS England takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material online without unreasonable "over-blocking"
- TASIS England recognises that students may choose to circumvent certain safety precautions by using devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management and additional staff/student training.

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets; please see Appendix 5 for more details): TASIS England operates as a mobile phone-free environment by default; anything other than this is by exception only, following a documented risk assessment. This applies equally to smart watches and smart glasses and any other technology or devices with similar functionality. Students may not use or access mobile phones during the school day (arrival to departure, including transitions, breaks, lunch, study halls and co-curriculars) and must adhere to the sectional arrangements in place for the storage and/or handing in of devices, as set out in Appendix 7 and as directed by their Section Head.

We keep this policy under equality review to ensure reasonable adjustments for students with SEND or other protected characteristics.

Recordings Made Using Mobile Electronic Devices: Using the camera on a phone or similar device, either to photograph/film/record any member of the school community, do any form of live streaming or to show to others the photos/videos/audio recordings already on the phone or similar device is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.

Cyberbullying: Cyberbullying is the use of IT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will not be tolerated, and incidents of cyberbullying should be reported and will be dealt with in accordance with the school's Anti-Bullying Policy.

Online Sexual Harassment: Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. online sexual harassment include: non-consensual sharing of nude or semi-nude images and videos and sharing sexual images and videos (the making or sharing of nudes and semi-nudes); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under our Child Protection Procedures. (Please see our Safeguarding Children Child Protection Policy for more details)

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g., for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at: The UK Safer Internet Centre provides an Online Safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. Providing expert advice and support for school staff regarding Online Safety issues and when an allegation is received.

If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will assess whether the

image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

We follow **UKCIS: *Sharing nudes and semi-nudes - advice for education settings***, including safeguarding-led responses, evidence preservation, and removal routes (e.g. via the IWF) where images are assessed as illegal.

Social Media, Including TikTok, Snapchat, Facebook, X and Instagram: TikTok, Snapchat**,** Facebook, X, Instagram and other forms of social media are increasingly becoming an important part of our daily lives. Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Head of School for reasons of work. Faculty/staff and students are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others. Staff and students are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever. Faculty, staff and students are aware that their online behaviour should always be compatible with UK law. Unauthorised use of personal social media accounts on school equipment could result in disciplinary action.

Online Forms of Abuse (Also see our Safeguarding Children Child Protection Policy): Information and communication technology (IT)-based forms of child physical, sexual and emotional abuse can include bullying via mobile phones or online (internet) with verbal and visual messages. This can also include child sexual abuse. All staff are alert to the signs that a child may be at risk of being, or may have been, abused online and will follow the school's child protection procedures (Please see our Safeguarding Children Child Protection Policy for more details).

IT-Based Sexual Abuse: The impact on a child of IT-based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. IT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response are recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with students, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Students are reminded that sending nude or semi-nude images is strictly prohibited by the school and may constitute a criminal offence. Described in KCSIE 2026 as the making or sharing of nudes and semi-nudes, the school will treat incidents of both sending and receiving these images as a safeguarding and/or child protection issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

There are no circumstances that will justify adults possessing indecent images of students. Adults who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making and storing indecent images of students is illegal. This will lead to criminal investigation and the individual being barred from working with students, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with students. Adults should ensure that students are not exposed to any inappropriate images or web links. Where indecent images of students or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

The Child Exploitation and Online Protection (CEOP) Tel: 0370 496 7622 Email: communication@nca.xgsi.gov.uk brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse. The main concern for teachers is the safe and effective supervision of students using the internet in school. The CEOP website is an invaluable source of information and resources concerned with Online Safety. However, many students now use the internet at home for homework and socialising, therefore the school will need to assist parents to understand the positive ways in which the internet can be used but also some of the associated risks. The website www.becta.org.uk clearly outlines the requirements of a school to control a student's internet viewing and enforce the school's Acceptable Use Policy.

Chat Room Grooming and Offline Abuse: Our faculty/staff need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of students online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Artificial Intelligence (AI): Generative artificial intelligence (AI) tools are now widespread and easy to access. Faculty, staff, students, and parents/carers may be familiar with generative chatbots such as ChatGPT and Copilot. TASIS England recognizes that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes,' where AI is used to create images, audio, or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. TASIS England will treat any use of AI to bully students in line with our Anti-Bullying and Behaviour Management policies. Faculty and staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out an appropriate risk assessment where new AI tools are being used by the school.

No personal or sensitive data about students, staff or families is to be entered into generative AI tools unless explicitly authorised following a Data Protection Impact Assessment and with appropriate safeguards in place. The school has regard to the DfE guidance 'Generative artificial intelligence in education' on the safety considerations and legal responsibilities that apply to teacher-facing and student-facing uses of AI, and to the DfE online resources on the safe and effective use of AI in education, published in partnership with the Chiltern Learning Trust and the Chartered College of Teaching.

Communicating and Educating Parents/Carers in Online Safety: We believe it is essential for parents/carers to be fully involved in promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and communicate with parents/carers to build a shared understanding of the benefits of new

technologies and the associated risks. Parents/carers are provided with a copy of the IT User Acceptance Policy (AUP). For PreK-Grade 5, parents/carers sign the AUP on the child's behalf; from Grades 5-12, students sign their own AUP and parents/carers receive a copy for information. TASIS England recognises the crucial role that parents play in the protection of their children with regards to Online Safety. The school organises annual awareness sessions for parents with regards to Online Safety, which look at emerging technologies and the latest ways to safeguard children from inappropriate content. The school will also provide parents and carers with information through newsletters, website; Parents/Carers sessions. Parents and carers are always welcome to discuss their concerns on Online Safety with the school, who can direct them to the support of our Online Safety Coordinator if required. Parents and carers will be encouraged to support the school in promoting good Online Safety practice.

- Parents/carers are required to decide as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- Parents/carers are expected to sign an agreement containing the following statement or similar:
- We will support the school approach to Online Safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school's name into disrepute.
- The school disseminates information to parents relating to Online Safety where appropriate in the form of posters , regular newsletters and school websites.

Taking and Storing Images of Students Including Mobile Phones (See our related documents including Appendix 6): TASIS England provides an environment in which students, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of students, or to take photographs of students apart from circumstances as outlined in Appendix 6 of this policy. This prevents staff from being distracted from their work with students and ensures the safeguarding of students from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere on the website, particularly in association with photographs. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g., mobile phone, tablet, laptop etc. The school has a Mobile Phone Policy which includes:
  - The commitment to keep the students safe.
  - How we manage the use of mobile phones at TASIS England taking into consideration faculty, staff, students on placement, volunteers, other professionals, trustees, visitors and parents/carers.
  - How we inform parents/carers, visitors and other professionals of our procedures.
  - What type of mobile phones will be used on educational visits and learning outside the classroom.
  - The consequences of any breaches of this policy.
  - Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

Filtering and Monitoring: The school provides a safe environment for students to learn and work, especially when online. Filtering and monitoring are both important parts of safeguarding students from potentially harmful and

inappropriate online material. The proprietor has overall strategic responsibility for filtering and monitoring. For this to occur, they have assigned a member of the Senior Leadership Team (the DSL) and the Chair of the Board of Directors to be responsible for ensuring these standards are met. The DSL works closely with the IT Manager and other members of SLT to ensure that filtering and monitoring is adequate and robust across the school and boarding facilities. The school considers those who are potentially at greater risk of harm and how often they access the school's IT systems. The school follows the current DfE Filtering and Monitoring Standards (June 2026) which ensure that the school:

- identifies and assigns roles and responsibilities to manage filtering and monitoring systems;
- reviews filtering and monitoring provision at least annually;
- blocks harmful and inappropriate content without unreasonably impacting teaching and learning;
- has effective monitoring strategies in place that meet the school's safeguarding needs.

Compliance with DfE Filtering and Monitoring Standards (June 2026)

We meet the Department for Education's standards by:

- **Roles & ownership:** The proprietor/Board holds strategic responsibility. The DSL is the senior operational owner and works with the IT Manager to run day-to-day controls.
- **Written monitoring strategy:** We maintain a documented monitoring strategy that is proportionate to risk and explains who/what is monitored, frequencies, alerting, and how safeguarding signals reach the DSL team for timely action.
- **Review cadence:** Leaders review filtering and monitoring at least once every academic year and after any significant change. Reviews are carried out by the SLT member responsible for filtering and monitoring, with the support of the DSL and IT support, and include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, with a record kept of these checks. Outcomes and actions are recorded.
- **Provider lists:** Our provider blocks illegal content using current **IWF** and **CTIRU** lists.
- **Change & exception logs:** All block/allow changes and curriculum exceptions are authorised, justified and auditable; logs are retained for at least 12 months (normally 24 months).
- **Training & awareness:** Relevant staff receive role-specific training, so leaders understand the systems in place and how to escalate concerns.
- **Proportionate privacy:** Monitoring is undertaken for safeguarding and security, is proportionate to risk, and is sign-posted in AUPs and privacy information.

The IT Team and DSL have worked together and ensured:
The filtering provider MUST be a member of the Internet Watch Foundation (IWF), signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and block access to illegal content including child sexual abuse material (CSAM).

- Any specific risks or vulnerable student groups are identified (age of students, SEND issues, EAL, PSHE, RSE, County Lines, Bring Your Own Device (BYOD) etc.)
- All existing school computers and devices are monitored and checked by the IT Team in association with the Sectional Safeguarding Teams. Boarding students are required to register their e-based devices and are required to use the school Wi-Fi system.

Cyber Security: The school recognises its responsibility to ensure that appropriate security protection procedures are in place to safeguard school systems. We work to the DfE's Cyber security standards for schools and colleges (June 2026), including multi-factor authentication (MFA) for remote/admin access, unique accounts with

least-privilege permissions, timely patching, tested offline backups, a defined incident-response plan, and staff awareness (e.g. phishing and reporting). As part of our whole-school Online Safety Training, we ensure faculty and staff, the Board of Directors, relevant Board sub-committees and Proprietor are updated with the evolving cyber-crime technologies. In addition, the school actively considers the Cyber security standards (DfE: June 2026) and uses these as a base for keeping the school and its community safe from cyber-crime**,** including the implementation of MFA where applicable, regular security audits, and staff training on cyber security. Additionally, we employ threat detection systems to monitor and protect against potential cyber threats.

Remote Learning (Please see our Remote Learning Policy for more details): Where there are periods in which the school is forced to close yet continue to provide education (such as a pandemic) it is important that TASIS England supports faculty, staff, students and parents to access learning safely, especially considering the safety of our vulnerable students. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Faculty, staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns and will act on concerns immediately. Any such concerns should be dealt with as per the Safeguarding Children Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Online teaching should follow the same principles as set out in the school's staff and students respective Behaviour - Code of Conducts. Additionally, TASIS England will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The school will put additional measures in place to support parents and students who are learning from home. This will include specific guidance on which programs the school is expecting students to use and how to access these alongside how students and parents can report any concerns that they may have. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our schools Remote Learning Policy.

Only approved school systems may be used for remote delivery. Platforms are risk-assessed, covered by appropriate data-processing agreements, and configured with privacy-protective settings. Staff use school accounts/devices wherever possible and follow the same filtering/monitoring and data-handling expectations as on-site.

Additionally, the Head of School has a duty of care for ensuring the safety (including Online Safety) of members of the school community, with the day-to-day responsibility being delegated to the Online Safety Lead who is our DSL. The Head of School and the DSL are aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of faculty/staff, which is in line with our main safeguarding reporting procedures. Staff working remotely should wherever possible use their school-issued IT equipment, however they may use their own computer equipment if this is not practical, as long as it is in accordance with the school's Data Protection Policy. Faculty and staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

For more information relating to Online Safety procedures, refer to the Online Safety Frequently Asked Questions (FAQ) in Appendix 5. It covers the following topics on the relevant page as follows:

- How will the policy be introduced to students? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents' support be enlisted?

- Why is the use of the Internet and IT important? How is the safe use of IT and the Internet promoted? How does the Internet and use of IT benefit education in our school? How will students learn to evaluate Internet content?
- How is filtering managed? How are emerging technologies managed? How to react to misuse by students and young people
- How is printing managed? What are the categories of cyberbullying? What are the student rules?
- What has research into cyberbullying found? What is the impact on a child of IT based sexual abuse? What is the impact on a child of IT-based sexual abuse? How do I stay secure on the Internet? Why is promoting safe use of IT important? What does the school's Mobile Phone Policy Include?
- Where can we learn more about Prevent? What do we have to do?
- Do we have to have a separate Prevent Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?
- What training must we have? What are the potential legal consequences if we do not take the Prevent duty seriously? What are the rules for publishing content online?

Related Documents:

- Online Safety Appendices.
- Safeguarding Children and Child Protection Policy; Anti-Bullying Policy; Behaviour Management, Discipline & Sanctions Policy.
- Prevent Duty: Tackling Extremism and Radicalisation Policy, Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE); The School Rules.
- Taking and storing images of students - Including Mobile Phones Policy; Acceptable use of IT Sign off forms for Staff/Students; Use of Photographs Sign-off Form.
- What to do if you are worried; https://www.ceopeducation.co.uk/.

Legal Status:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5 January 2015 and as amended in September 2015
- *Keeping Children Safe in Education* (KCSIE) *Information for all schools and colleges* (DfE: September 2026) incorporates the additional statutory guidance.
- *National Minimum Standards for Boarding Schools* (DfE: May 2026), which apply to the school's boarding provision, including boarders' access to the internet and electronic devices.
- *Statutory framework for the Early Years Foundation Stage* (September 2026) - Section 3 (safeguarding and welfare requirements) is read alongside KCSIE 2026 in respect of children in the Early Years.
- *Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.*
- *Working Together to Safeguard children* (WT) (HM Government: 2026) which also refers to non-statutory advice, *Information sharing* HM Government: May 2024); *Prevent Duty Guidance: for England and Wales* (2023, as updated) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for schools and childminders (DfE: 2023, as updated)*
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'
  - Prepared with reference to DfE Guidance (2017) *Preventing and Tackling Bullying: Advice for Advice for headteachers, staff and governing bodies*
  - Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*

- The Data Protection Act 2018; UK GDPR (each as amended by the Data (Use and Access) Act 2025) and Child Exploitation and Online Protection Command (CEOP).
- Teaching Online Safety in Schools (DfE: 2023)
- The policy also takes into account the National Curriculum computing programmes of study.
- Meeting digital and technology standards in Schools and Colleges (DfE: June 2026) (including Broadband, Cyber-Security and data protection procedures)
- Filtering and monitoring standards for schools and colleges (current DfE digital and technology standards) (June 2026)
- Cyber security standards for schools and colleges (current DfE digital and technology standards) (June 2026)
- Promoting and supporting mental health and wellbeing in schools and colleges (September 2021 - updated July 2025)
- Behaviour in schools (February 2024)

Guidance (UK Safer Internet Centre)

- Test Your Internet Filter (UKSIC / SWGfL)
- A Guide for education settings and filtering providers (UKCIS)
- Establishing appropriate levels of filtering (UKSIC)
- Online safety in schools and colleges: questions from the governing board (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people

Appendix 1: Early Years Online Safety, Internet and Acceptable Use Policy

The Pre K to Grade 4 Acceptable Use policy is available as an online form at this link: Pre K to Grade 4 Enrolment forms

This policy, which applies to the whole school inclusive of the Early Years Foundation Stage, is in support of the health and safety policy and the individual health and safety assessments. This policy is publicly available on the school's website. On request a copy may be obtained from the school's office

Aim: The Acceptable Use Policy (AUP) will aim to:

- Safeguard students and young people by promoting appropriate and acceptable use of information and communication technology (IT).
- Outline the roles and responsibilities of all individuals who are to have access to and/or be users of work-related IT systems.
- Ensure all IT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

Scope: The AUP will apply to all individuals who are to have access to and/or be users of work-related IT systems. This will include students and young people, parents and carers, the Early Years teacher and their teaching assistants, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive. Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of IT that takes place on-site, and, where known, off-site.

Roles and responsibilities:

Early Years: The Head and Deputy Head of Pre K to Grade 8 have responsibility for ensuring Online Safety in Pre K to Grade 8 including Early Years and is an integral part of everyday safeguarding practice. The Head and Deputy Head of Pre K to Grade 8 will liaise with the DSL and Online Safety Coordinator who will monitor the practice of Online Safety within the Early Years. This will include ensuring:

- The Early Years teacher and their teaching assistants will receive the appropriate training, guidance, time and resources to effectively implement Online Safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal IT equipment by all individuals who affect or come into contact with the Early Years setting. Such policies and procedures are to include the personal use of work-related resources.
- The AUP is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be open and transparent.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection.

Designated Safeguarding Lead (DSL): The DSL must be a senior member of the leadership team who is to have relevant, current and practical knowledge and understanding of safeguarding, child protection and Online Safety. Access to an individual holding this role is to be available at all times, for example, a Designated Deputy. The designated person for safeguarding will be responsible for ensuring:

- Agreed policies and procedures are to be implemented in practice.
- All updates, issues and concerns are to be communicated to all IT users.
- The importance of Online Safety in relation to safeguarding is to be understood by all IT users.
- The training, learning and development requirements of the Early Years teacher and their teaching assistants are to be monitored, and additional training needs identified and provided for.
- An appropriate level of authorization is to be given to IT users.

Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of students and young people will address Online Safety. A safe IT learning environment is to be promoted and maintained.

Early Years teacher and their teaching assistant: The Early Years teacher and their teaching assistant will ensure:
- The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
- IT equipment is to be checked before use and all relevant security systems judged to be operational.
- Awareness will be raised of any new or potential issues, and any risks which could be encountered as a result.
- Students and young people are to be supported and protected in their use of online technologies - enabling them to use IT in a safe and responsible manner.
- Online safety information is to be presented to students and young people as appropriate for their age and stage of development.
- Students and young people will know how to recognize and report a concern.
- All relevant policies and procedures are to be adhered to at all times and training undertaken as is to be required.

Students and young people: Students and young people will be encouraged to:
- Be active, independent and responsible learners.
- Abide by the Acceptable Use Agreement as to be approved by peers, the Early Years teacher and their teaching assistant, parents and carers.
- Tell a familiar adult about any access to inappropriate content, material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand (age and activity dependent).

Acceptable use by the Early Years teacher and their teaching assistant: the Early Years teacher and their teaching assistant should be enabled to use work-based online technologies:
- To access age-appropriate resources for students and young people.
- For research and information purposes.
- For study support.

Use of images, displays etc: We will only use images of our students for the following purposes:
- Internal displays (including clips of moving images) on digital and conventional notice boards within the school premises,
- Communications with the school community (parents, students, faculty, staff), for example newsletters.
- Marketing the school both digitally by website, by prospectus [which includes an iPad app], by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

In the event of misuse by the Early Years teacher or their teaching assistant: Should it be alleged, that an Early Years practitioner or manager is to have misused any IT resource in an abusive, inappropriate or illegal manner, a report is to be made to the Head of School or Designated Safeguarding Lead immediately. Should the allegation be made against the Head of School or Designated Safeguarding Lead, a report is to be made to a member of the Senior Leadership Team. Procedures are to be followed as appropriate, in line with the Acceptable Use Policy, Safeguarding Children Child Protection Policy and/or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.

Acceptable use by students and young people: Students and young people will also be informed of the behaviours, which will be deemed unacceptable. This will allow students and young people to take some degree of responsibility for their own actions. Students will only be able to download a file under the direct supervision of a member of staff and it will be virus checked prior to being opened. The use of game-style activities and websites should be monitored by teachers to determine suitability.

Acceptable use by visitors, contractors and others: All individuals who affect or come into contact with the Early Years setting are to be expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with students and young people. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved.

Links to other policies:

Behaviour Management, Discipline & Sanctions Policy: The Behaviour Management, Discipline & Sanctions Policy together with the Anti-Bullying (Countering Bullying) Policy contain up-to-date anti-bullying guidance, which should highlight relevant issues, such as cyberbullying. It should be recognised that all inappropriate behaviours will be taken seriously and dealt with in a similar way, whether committed on or offline. There are to be consistent expectations for appropriate behaviour in both the 'real' and 'cyber' world and this is to be reflected in all relevant policies.

Safeguarding Children Child Protection Policy and Acceptable Use Policy: The Safeguarding Children Child Protection Policy and the Acceptable Use Policy are to be referred to when dealing with any incidents that should occur as a result of the intentional or unintentional misuse of IT. Any allegations of abuse or other unlawful activity are to be reported immediately to the Designated Safeguarding Lead who will ensure procedures outlined in the Safeguarding Children Child Protection Policy are followed with immediate effect.

Relationships and Sex Education Policy: When teaching students about developing positive relationships and sex education, including Health Education, this is underpinned by teaching effective Online Safety practices alongside how to report online sexual harassment or unwanted content.

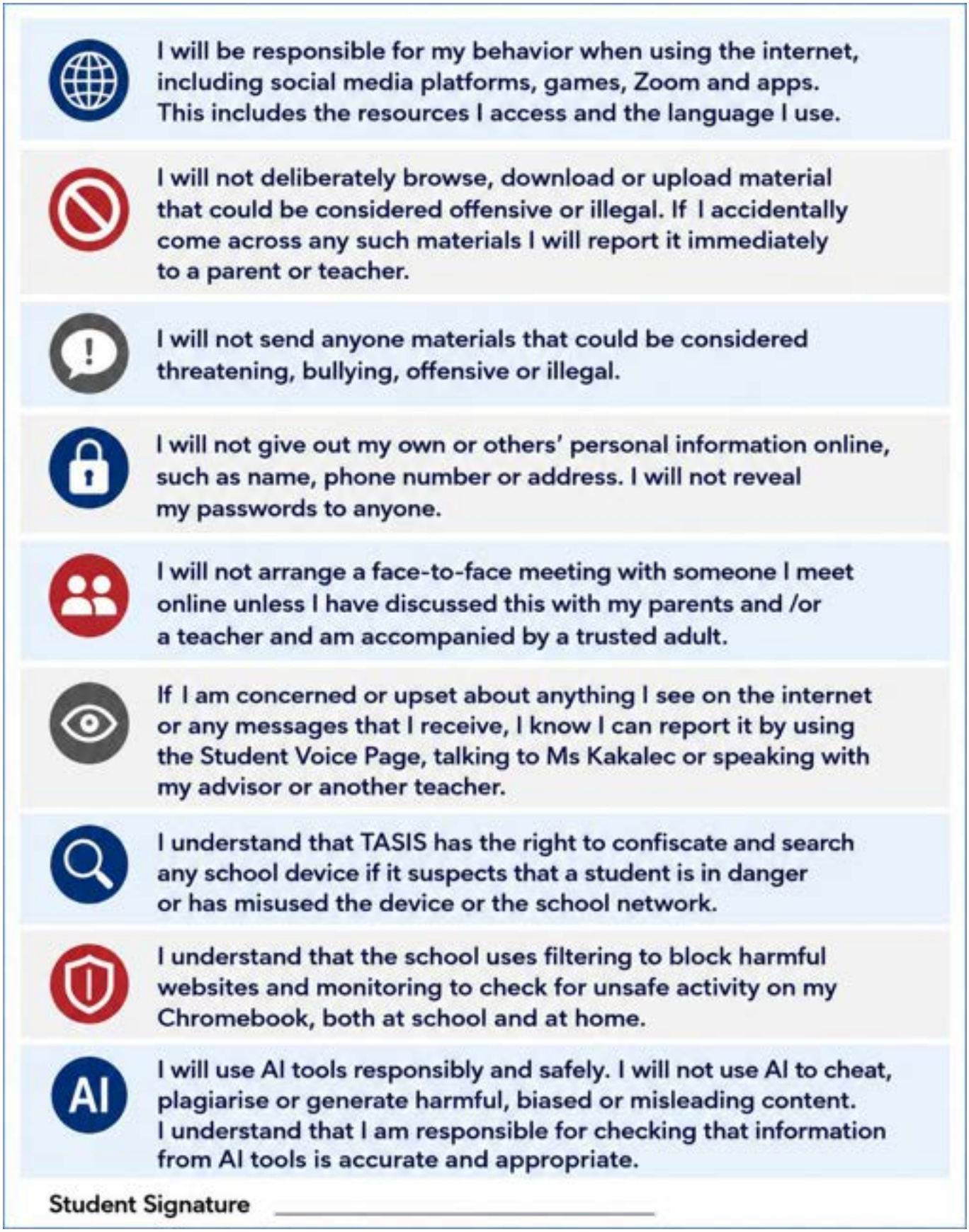
Personal, Social, and Emotional Development: The promotion of Online Safety within PSED activities is to be considered essential for meeting the learning and development needs of students and young people. Key messages to keep students and young people safe are to be promoted and should be applied to both online and offline behaviours.

Health and Safety Policy: The safe use of IT is included within the Health and Safety Policy and should also include guidelines for the use of display screen equipment. The detrimental impact of prolonged IT use on students' brain development should also be addressed.

Appendix 2: Grade 5 to Grade 8 and Upper School Students Acceptable Use of IT Equipment

E	**Ensure that I do not create, send or post anything which is offensive to other people or brings the school into disrepute. I will not use any language or images which could offend any minority or cultural groups.**
S	**Secure all my passwords and not share them with others. I understand I must not reveal or use anyone else's login details or access a device someone else is logged onto. I will change my password immediately if it becomes known to someone else and ensure I log out after every network session.**
A	**Access only appropriate material. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that school can monitor my use of the internet. I will report any accidental access to other people's information, unsuitable websites or receipt of any inappropriate material as well as any security risk or suspicious behaviour that I become aware of. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity.**
F	**Facebook, social media and email use. I will not publish my own and others' personal details, information or location over any social networking site. I am aware that email is not guaranteed to be private. Messages or any communication via social media or email supporting illegal activities will be reported to the authorities.**
E	**Exercise caution when downloading material. I understand that the illegal download and/or copyright of any material, including receiving, sending or publishing, is forbidden any may be passed to the relevant authorities. I will not download any unapproved software, system utilities or resources from the internet.**
T	**Turn off mobile hotspots and not use the network in any way that will disrupt its use for other people. This includes any attempt to harm, destroy or remove any equipment, work of another user, or website connected to the system. Mobile hotspots could be disabled via the WiFi network.**
Y	**Your device, your responsibility. I understand that the school has the right to confiscate and search any device if it suspects that a student is in danger or has misused a device or the school network. I understand that any activity from a device I own is my responsibility, including all portable devices and their content or viruses.**

Example Student Acceptable Use Policy - Grades 5-8



I will be responsible for my behavior when using the internet, including social media platforms, games, Zoom and apps. This includes the resources I access and the language I use.

I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such materials I will report it immediately to a parent or teacher.

I will not send anyone materials that could be considered threatening, bullying, offensive or illegal.

I will not give out my own or others' personal information online, such as name, phone number or address. I will not reveal my passwords to anyone.

I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and /or a teacher and am accompanied by a trusted adult.

If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can report it by using the Student Voice Page, talking to Ms Kakalec or speaking with my advisor or another teacher.

I understand that TASIS has the right to confiscate and search any school device if it suspects that a student is in danger or has misused the device or the school network.

I understand that the school uses filtering to block harmful websites and monitoring to check for unsafe activity on my Chromebook, both at school and at home.

AI

I will use AI tools responsibly and safely. I will not use AI to cheat, plagiarise or generate harmful, biased or misleading content. I understand that I am responsible for checking that information from AI tools is accurate and appropriate.

Student Signature _____

All students must follow the rules outlined in this policy when using school IT resources and equipment, including all Internet access and the Learning Management System (LMS), accessed from both in and outside of school, and on school provided or personal electronic devices. Breaking these conditions may lead to confiscation of any electronic devices, close monitoring of the student's network activity, investigation of the student's past network activity, withdrawal of the student's access and, in some cases, permanent removal from the school and even criminal prosecution. Students are also expected to take care of school-issued electronic devices and any damage to them may result in fines to replace or fix damaged devices. Misuse of the Internet will be dealt with in accordance with the school's Behaviour Management, Discipline & Sanctions Policy and, where there is a safeguarding risk, the Safeguarding & Child Protection Policy. The school is not responsible for any loss of data on the network; computers connected to the network or data storage used on the network (including USB memory sticks). Data held on the network will be backed up for a limited period. Students are responsible for backups of any other data held. Use of any information obtained via the network is at the student's own risk.

Students are expected to use the network systems in a responsible manner and to use the resources for the educational purposes for which they are provided.

It is not possible to compile a complete set of rules about what is, and what is not, acceptable; however, the above should be a guide and in cases of dispute the decision of the Head of School will be final.

Student agreement:

I agree to follow the school rules on the use of school network resources and mobile electronic devices. I will use the network and all mobile electronic devices in a responsible way and observe all the conditions explained in both the Online Safety Policy and this Acceptable Use Policy. I understand and accept the consequences of breaking these rules.

Print student name .....

Student Signature .....

Parent/Guardian agreement:

I understand that my child has agreed to accept the terms of the Online Safety and Student AUP Policy, and I confirm that I accept the terms of the agreement. If my child brings any personal electronic devices to school, I understand that the student is responsible for its safekeeping and appropriate usage while in transit to and from and on campus.

I have read and understood the Online Safety Policy and agree to check any updates, which are made available on the Parent Portal.

Print Parent/Guardian name .....

Parent/Guardian Signature .....

Date .....

Appendix 3: Acceptable Use of IT Sign-off Form for All Faculty and Staff at TASIS England

To ensure that members of faculty and staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the school's Online Safety Policy and IT Acceptable Use Policy for further information and clarification. You must not use any IT on-site until you have signed this Code of Conduct document and logged it with HR.

- I will respect all IT equipment/facilities at TASIS England and will report any faults that I find or any damage that I accidentally cause.
- I agree to abide by this policy in respect of any of my own IT equipment or mobile devices that I bring on site. If any IT device (personal or school-issued) is being used inappropriately or illegally on site (or inappropriately in the presence of students), the Section Head may request that the device be monitored. Failure to comply with the monitoring could result in informing the appropriate authorities.
- I understand that no photographs of students may be taken with or stored on my personal electronic devices, including cameras, iPads, mobile phones, or personal computers.
- Photos of students should not be uploaded to personal social media accounts
- I am familiar with the school's Data Protection Policy, and I agree I am responsible for the security of all personal data in my possession. I agree that all personal data that relates to an identifiable person and is stored or carried by me on a removable memory device will be encrypted or contained within password-protected files to prevent unauthorised access.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others then I will immediately ask for these details to be changed.
- I agree that my use of TASIS England IT equipment/facilities will be monitored and may be recorded at all times. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on-site or using TASIS England equipment/facilities. I understand that I may temporarily access blocked websites, services and other online resources using only tools that are provided by TASIS England. I agree not to display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.
- I agree that the provision of TASIS England IT equipment/facilities including the email and Internet system are for educational purposes, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other clauses in this document.
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of IT on-site or using TASIS England equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not deliberately view, send, upload or download any material that is unsuitable for the school environment whilst I am in that environment or using any IT equipment/facilities belonging to TASIS England. If I accidentally encounter any such material then I will immediately close, but not delete in the case of emails, the material and immediately report it to the Online Safety Coordinator or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents I will help to improve Online Safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the Online Safety Coordinator. I will not access any material that the Online Safety Coordinator has rated as unsuitable.
- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using TASIS England equipment or facilities. If I disclose any additional personal details contrary to this instruction, then I agree that these details can be recorded and that I will not hold TASIS England responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times. I recognise that staff should not communicate with students through personal electronic devices or methods such as social networking sites, blogging, chat rooms, text messaging, messenger applications or private email. Instead, only the school email system may be used.
- Staff are expected to enable Multi-Factor Authentication (MFA) for the Google Workspace and Axiom/LMS.

Signed:_____ Date:_____

Appendix 4: Whole School Mobile and Smart Technology Policy, including taking and storing images of students

Legal Status: This policy was prepared with reference to KCSIE (DfE: September 2026), Ofsted advice on the use of mobile phones for the Early Years, the Department for Education's published guidance on the use of mobile phones (Mobile phones in schools, statutory guidance to be followed from 1 September 2026) and UK law governing the use of mobile phones while driving.

Applies to:

- The whole school including the Early Years, co-curricular program, school trips, Summer School and Summer Camps and all other activities provided by the school, inclusive of those outside of the normal school hours.
- All staff (teaching and support staff), students on placement, the Board of Directors and volunteers working in the school.

Related documents (available on the school website):

- Safeguarding Children and Child Protection Policy
- Behaviour Management, Discipline and Sanctions Policy
- Anti-Bullying (Countering Bullying) Policy

Availability: This policy is made available to parents, faculty, staff and students in the following ways: via the school website, parent portal and on request, a copy may be obtained from the Office.

Monitoring and Review:

- This policy will be subject to continuous monitoring, refinement and audit by the Head of School.
- The Head of School undertakes a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed: Date:

Head of School

Introduction: Whilst we understand the use of mobile phones and cameras for educational purposes and the convenience they offer and recognise that learning to use digital technology is an important part of the IT and wider curriculum, equally we must ensure the safeguarding needs of the students are met and staff, parents and volunteers are not distracted from their care of students. Mobile phones, alongside other technologies, aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are associated risks. Students and young people must be encouraged to understand such risks, to enable them to develop the appropriate strategies which will keep them safe.

Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses as to be agreed with the Designated Safeguarding Lead. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

Aims: The aim of the Mobile Phone Policy is to protect students and young people from harm, by ensuring the appropriate management and use of mobile phones by all individuals who work or visit our school. Students and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use. This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

Scope: The Mobile Phone Policy will apply to all individuals who are to have access to and or be users of personal and/ or work-related mobile phones within the broadest context of the setting environment. This will include students and young people, parents and carers, the Early Years teacher and their teaching assistants, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

Policy statement: It is to be recognised that it is the enhanced functions of many mobile phones that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and cyberbullying. It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to students and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

Code of conduct: A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the students and young people in their care. It is to be ensured that all teachers and teaching assistants will:

- Be aware of the need to protect students from harm.
- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Be vigilant and alert to potential warning signs of misuse.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Be responsible for the self-moderation of their own behaviours.
- Be aware of the importance of reporting concerns immediately.

It is to be recognised that studies consistently indicate that imposing rigid regulations and/or 'bans' on the actions of others are counterproductive and should be avoided. Such imposition will lead to a culture of suspicion, uncertainty and secrecy. An agreement of trust is therefore to be promoted regarding the carrying and use of mobile phones within the school. This is to

be agreed by all service users, including all students, young people and adults who are to come into contact with the school setting.

Guidance on use of mobile phones by teaching staff including those in the Early Years: The following points apply to all staff and volunteers at our school including those who teach in the Early Years Foundation Stage and apply to the use of all mobile devices to ensure the quality of supervision and care of the students, as well as the safeguarding of students, staff, parents and volunteers in the school.

TASIS England allows staff to bring in mobile phones for their own personal use. However, they must be kept away in closed drawers or their bags at all times and are not allowed to be used in the presence of students (this includes not using them in silent mode while students are in the classroom, i.e., during a test or quiz). They may be used during working hours in a designated break away from the students. Staff are not permitted to use recording equipment on their personal mobile phones to take photos or videos of students. If staff fail to follow this guidance, disciplinary action will be taken in accordance with TASIS England Disciplinary Policy. During outings nominated staff will be permitted to have access to their own mobile phones, which are to be used for emergency contact only. During off-campus activities, i.e., field trips and overnight excursions, trip leaders will be provided with a school-issued mobile phone in good working condition.

Any other member of staff working within Early Years must ensure that they do not bring any other personal devices into classes. In the Early Years setting, school IT (i.e., iPads. iPods and digital camera) will be used to evidence the students' personnel and learning development for the student.

There are iPads with access to Wi-Fi owned by the school for the specific education purposes.

If staff need to make an emergency call, (such as summoning medical help or reporting an intruder on the premises) they must do so irrespective of where they are, via their own mobile phone or a school phone. Staff should provide the school number to members of the family and next of kin so in an emergency the member of staff can be contacted on the school phone.

There are film and digital cameras available for staff to use. Faculty/staff must ensure that there is no inappropriate or illegal content on their phones or mobile devices. Should any member of staff become aware of inappropriate or non-essential use of a mobile phone, this should be reported to a member of the Senior Leadership Team and may be subject to disciplinary action.

Early Years and SeeSaw portfolios: Photographs taken for the purpose of recording a child or group of students participating in activities or celebrating their achievements is an effective form of recording their progression in Early Years and other areas of the school. However, it is essential that photographs are taken and stored appropriately to safeguard the students in our care. When students join our school, we ask parents to sign consent for photographs and videos to be taken for such purposes.

All teachers are responsible for the storage of school cameras, which should be locked away securely when not in use. Images taken and stored on school cameras should be downloaded onto their school-issued computer and deleted from the cameras. Staff are not to use their own equipment to take photos of students. Under no circumstances must cameras of any kind be taken into the toilets (this includes any device with photographic or video capabilities). In the Early Years, photographs are sometimes distributed to members of key workers to record in students' profiles. Staff are not permitted to make extra copies of the photographs in any format.

Photographs are also taken at group events and activities and displayed around the child's room and in photograph albums for all the students to look back on and to talk about with their friends and teachers about the events that have happened in the Early Year. For this we need to have written parental permission for photo release that is requested upon enrolment. Every parent has the right to refuse this request, in which case the child must not be photographed by any member of staff, by a parent, or by any outsider without the express permission for that occasion of the parent with whom the Early Years has a contract.

Storage and review of images: Images of students are stored securely. Digital photographs and videos are reviewed annually and are deleted when no longer required. We regularly check and update our web site, when expired material is deleted.

TASIS England school website and social media platforms: Photographs and videos may only be uploaded to the school's website or official social media pages with the Head of School's approval. Student's surnames are never used on our website, or social media pages. When students join TASIS England, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld such photographs/videos are not published of the individual child concerned. Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

External photographers: Professional photographs are taken throughout the year at school shows, by local media and Professional School Portraits. The Head of School ensures that professional photographers are DBS checked and that they have their own stringent regulations, which ensure safeguarding of students from inappropriate use of images.

Appropriate use of a mobile phone during the school day (including social networking): School-issued mobile phones have a place on outings or in school buildings, which do not have access to a school landline. In these cases, they are often the only means of contact available and can be helpful in ensuring students are kept safe. Ideally staff should use school mobile phones in these circumstances but, if required to use a personal phone, should input 141 to ensure their own number is hidden.

When leaving the school building with students (e.g., for sport, or on school trips), the school issued mobile phones must be switched on and turned to loud to ensure that staff can be contacted by the school. Contact numbers for all members of staff accompanying the students must be left at Reception and a list of contact telephone numbers for all students should be with the leader of the off-site activity (although these must be kept confidential).

Faculty/staff must not post anything onto social networking sites such as Facebook that could be construed to have any impact on the organisation's reputation. (We advise all our staff to carefully restrict their Facebook profiles to ensure they cannot be contacted by parents and students; this could involve removing their last name from their page). We explain to staff that although they are able to accept friendship requests from friends who may also be parents of students at the school, staff must be aware of the potential issues this could cause. Faculty/staff must not post anything onto social networking sites that would offend any other member of staff or parent using the setting. If any of the above points are found to be happening, then the member of staff involved will face disciplinary action, which could result in dismissal. Where email contact is initiated by students who have graduated from TASIS England, TASIS England employees may reply from a TASIS England email address only with blind copies to line managers **and** the DSL.

We advise faculty and staff not to accept friend requests from students until graduates have been out of school for three years.

Students and mobile phones (mobile data access): TASIS England recognises that personal mobile devices can provide unrestricted access to the internet through mobile data and may bypass the School's filtering and monitoring systems. This can expose students to safeguarding risks including harmful or inappropriate content, bullying and harassment, the sharing of nudes and semi-nudes, pornography, exploitation and other forms of online harm. Students must therefore comply with the School's mobile-phone arrangements throughout the school day.

Grades 5–10: Students in Grades 5–10 may not use or access mobile phones or equivalent smart devices during the school day, including during lessons, movement between lessons, breaks, lunch, study periods and co-curricular activities. Devices must be switched off and stored securely in accordance with the arrangements specified by the relevant Section. A device must not be accessed simply because it is being carried in a school bag or stored in a locker. Exceptions may be authorised for an individual student where required for medical reasons, disability or SEND, safeguarding, travel arrangements or another specifically approved purpose.

Grades 11–12: Students in Grades 11–12 may retain possession of their mobile phones during the school day but must keep them switched off and securely stored. They may not use or access their phones during the school day, including during lessons,

transitions, breaks, lunch, study halls, free periods or co-curricular activities. Any exception must be specifically authorised by the Head of Upper School for a defined purpose, time and, where applicable, location. Misuse or unauthorised access will be dealt with in accordance with the Behaviour Management, Discipline and Sanctions Policy.

Boarding students: During the teaching day, boarders follow the same arrangements as day students in their grade. Outside the teaching day, mobile phones may be used during agreed periods of free time in accordance with Boarding routines. Phones must not interfere with sleep, supervision, study, activities, relationships or the privacy and welfare of others. Mobile phones are not normally used after lights out. Phones will be collected from younger boarders, ordinarily up to Grade 10, and this arrangement may be extended where a student persistently uses a device at inappropriate times. Because TASIS England is an international community, Boarding staff may agree proportionate arrangements for private family contact where international time zones make normal contact times impracticable.

Any use of mobile technology to intimidate, bully, harass, threaten or attempt to radicalise others or breach copyright laws will be counted as an infringement of network use and breach of discipline and will be dealt with in accordance with the school's Behaviour Management Discipline and Sanctions Policy. This may result in disconnection from the school network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, school and statutory guidelines are not breached.

Students are reminded that making, sending, requesting, receiving or sharing nude or semi-nude images or videos involving a child under 18 is prohibited by the School and may constitute a criminal offence. All incidents involving the sharing of nudes or semi-nudes, whether consensual or non-consensual, will receive a safeguarding response. Students who are concerned about images they have received, sent, requested or shared should speak to a member of staff immediately. The School will respond in accordance with KCSIE 2026 and the UKCIS Sharing nudes and semi-nudes guidance.

The School may confiscate mobile electronic devices in accordance with its Behaviour Management, Discipline and Sanctions Policy and the DfE's Searching, Screening and Confiscation guidance. Where an electronic device has been lawfully confiscated following a search, authorised staff may examine data or files on the device where there is good reason to do so and may retain, delete or pass material to the police where permitted by the statutory guidance. Safeguarding concerns will be referred to the DSL and managed in accordance with the Safeguarding Children and Child Protection Policy.

Use of images, displays etc: We will only use images of our students for the following purposes:

- Internal displays (including clips of moving images and yearbooks) on digital and conventional notice boards within school premises.
- Communications with the TASIS England community (parents, students, staff), for example newsletters.
- Marketing TASIS England both digitally by website, by prospectus [which includes a DVD and YouTube channel], by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

Images that we use in displays and on our web site: The images that we use for displays and communications purposes never identify an individual student. Instead, they name the event, the term and year that the photograph was taken (for example, 'Sports Day, Summer Term 2023'). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context. We never use any image that might embarrass or humiliate a student. Students are always properly supervised when professional photographers visit TASIS England. Parents are given the opportunity to purchase copies of these photographs.

The students take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents present often take photographs of these memorable events, which may include groups of students. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents.

Media coverage: We will always aim to notify parents in advance when we expect the press to attend an event in which our students are participating and will make every effort to ensure that images including students whose parents or guardians

have refused permission for such images of their students to be used are not used. We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the students of celebrities.

Staff induction: All new teaching and office staff are given guidance on the school's policy on taking, using and storing images of students.

Use of mobile phones for volunteers and visitors: Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of students. If faculty/staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school. The exception to this would be at an organised event. Faculty/staff should remind parents regularly of school policy regarding mobile phone use with the following statement on weekly emails, when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g., a family album) and so are exempt from the Data Protection Act 2018. Please be aware these images (which may include other students) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of the Act." If they wish to make or take an emergency call, they may use the office and the school phone.

Parental use of mobile phones/cameras within the school buildings: The growth of hand-held mobile technology and interconnectivity has implications for the safety of students, so in order to reflect the policy on safeguarding and child protection, it is essential parents do not use their mobile phones/cameras in the school building, apart from circumstances as outlined within Appendix 6 below. Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of students or in public areas of the school such as during meetings and school events.

The school records images of students, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of students while performing and disturbance within the audience.

Other mobile technology: At TASIS England, we recognise the value of mobile technology within our curriculum and our students' accommodation. Within the upper school, students are required to bring their own devices to support their studies. Any personal device that students bring to the school must be used appropriately in line with the Students' Acceptable Use Policy and must be kept securely. Where a student is found to be misusing a school or personal device, or accessing inappropriate content, the device may be confiscated by the school and appropriate action taken. When accessing the school Wi-Fi, staff, students and parents (for guest Wi-Fi access) must adhere to their IT Acceptable Use Policy (which includes downloading and running Content). Staff, students, volunteers and parents are responsible for their own mobile devices, and the school is not responsible for theft, loss, or damage.

Driving and the law: The use of hand-held phones while driving, whether to make or receive a call, is prohibited. The only exception to this will be in the event of a genuine emergency call to 999 or 112, if it would be unsafe for the driver to stop. Hand-held mobile phones used with an earphone and microphone are covered under the ban, as they still require the user to hold the phone to press buttons or to read a message on the phone's screen.

The Board and employees of the school will not require any employee to receive or make calls on a mobile phone while driving. Mobile phones must instead be directed to the message/voicemail service while driving.

The Head of School will not assist in the payment of any fine levied against anyone using a hand-held mobile phone while driving. An employee will be regarded as driving if the engine is running, even if the vehicle is stationery. Notification of any contravention of these requirements may be regarded as a disciplinary matter.

Appendix 5: Online Safety FAQs

How will the policy be introduced to students?

- Rules for Internet access will be posted in all rooms where computers are used
- Students will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- A module on responsible Internet use will be included in the PSHE program covering both home and school use.
- Students will be informed that network and Internet use will be monitored and appropriately followed up.
- Students will be made aware of the acceptable use of technology and sign upon enrolment

How will IT system security be maintained?

- The school IT systems will be reviewed regularly with regard to security
- Security strategies will be discussed at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work should be kept confidential by staff and not used in public computers.
- Files held on the school network will be regularly checked
- All network system and administration passwords are to be recorded by the IT Department and kept in a secure place with regular updates

How will faculty/staff be consulted and made aware of this policy?

- All faculty/staff must accept the terms of the 'Responsible Internet Use' statement included in the faculty handbook before using any Internet resource in school.
- All new faculty/staff will be taken through the key parts of this policy as part of their induction.
- All faculty/staff including teachers, learning support assistants and support staff will be provided with the School Online Safety Policy and have its importance explained as part of the child protection training requirement.
- Faculty/staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Faculty/staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Breaching this Online Safety policy may result in disciplinary action being taken and access to IT being restricted or removed.
- Faculty/staff will read and sign *Staff Code of Conduct for IT*- prior to using school IT equipment in the school
- Faculty/staff will always use a child friendly safe search engine when accessing the web with students.

How will complaints regarding Internet use be handled?

- Responsibility for handling complaints that have progressed to Stage 2 will be delegated to a relevant member of the Senior Leadership Team.
- Complaints of Internet misuse will be dealt with by the Head of School.
- Any complaint about staff misuse must be referred to the Head of School.
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children Child Protection Policy and procedures.
- Students and parents will be informed of the complaint procedure which is available on the TASIS England website.
- Parents and students will need to work in partnership with staff to resolve issues.
- As with drug issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the responsible Internet use policy in newsletters, the parent portal and on the school website.

- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach will be encouraged with parents and could include information booklets, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- We will maintain a list of Online Safety resources for parents.
- Parents will be invited to attend an Online Safety workshop annually.

Why is the use of the Internet and IT important? Not only is familiarity with the use of IT equipment a core requirement, but the efficient use of the equipment and available resources is also considered key - for example, the use of email for efficient communication and the correct use of the Internet for research. Staff across the school are making increased use of IT, which benefits not only the quality of teaching and support services but also their professional development. It is equally important that staff are properly equipped and supported to make the most efficient use of IT resources. In particular, IT is extremely beneficial in engaging our students, who have learning and physical disabilities. It can also help them to access parts of the curriculum, which they might not otherwise be able to engage with.

All students deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" IT facilities including online resources and services. Internet use is a part of the statutory curriculum and a necessary tool for staff and students. The school has a duty to provide students with quality Internet access as part of their learning experience. In order for the school to maintain such an environment for learners (students and adults) everybody must be aware of the need to ensure online protection (Online Safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

How is the safe use of IT and the internet promoted? TASIS England takes very seriously the importance of teaching students (and staff) to use IT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of IT in school, but also outside school in the wider community. TASIS England has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and TASIS England will further promote safe use of IT and the Internet by educating students and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and students complies with copyright law. TASIS England will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's IT education and is also embedded in our PSHEE, RSE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferInternet.org.uk)
- CEOP's Thinkuknow website (https://www.ceopeducation.co.uk/)

How does the Internet and use of IT benefit education in our school?

- Students learn effective ways to use IT and the Internet including safe and responsible use.
- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between students worldwide.
- Access to experts in many fields for students, faculty and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with LA and DfE
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will students learn to evaluate Internet content?

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.
- Students will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the teacher, DSL, Online Safety Coordinator or IT Department.
- Staff and students should ensure that their use of Internet derived materials complies with copyright law
- Students should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright.

How is filtering managed? Having Internet access enables students to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. Unsuitable and harmful online content is managed through the School's filtering and monitoring systems, which are configured according to safeguarding risk, the age and needs of students and the requirements of teaching and learning. In addition, students' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our IT Department. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of students. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some students may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at TASIS England we believe that the benefits to students having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of minors along with TASIS England share the responsibility for setting and conveying the standards that students should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide students towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

Steps for managing filtering:

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable online materials, they must report it to the DSL or IT Manager immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect students from unsuitable material and the methods used will be reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (https://www.iwf.org.uk/).

How are emerging technologies managed? IT now touches almost every aspect of students' lives. New and emerging technologies enhance communication and learning but also introduce new risks. We keep this list under annual review, so our controls, education and filtering/monitoring remain proportionate.

Examples (non-exhaustive) of technologies students use in and out of school include:

- Internet access and web browsing (**including search engines and AI-augmented results**)
- Email
- Instant messaging and group chats (e.g. **iMessage, WhatsApp, Telegram, Signal**)
- Community platforms and forums (e.g. **Discord, Reddit**)
- Social media platforms (e.g. **Instagram, Snapchat, TikTok, Facebook, X**)
- Live-streaming and short-form video (e.g. **TikTok Live, YouTube Live, Twitch, Instagram Live**)
- Video-sharing/hosting services (e.g. **YouTube, Vimeo**)
- Blogging and microblogging; podcasts and audio platforms
- Online gaming and in-game voice/text chat (e.g. **Roblox, Fortnite, Steam; PlayStation/Xbox/Nintendo online**)

- Cloud collaboration and file-sharing (e.g. **Google Workspace/Drive, Microsoft 365/Teams, Dropbox**)
- Photo and cloud storage services (e.g. **iCloud Photos, Google Photos**)
- Location sharing/tracking features (e.g. **Snap Map, Find My, Life360**)
- Mobile devices and connectivity features (e.g. **personal hotspots/tethering; Bluetooth/AirDrop/Nearby Share**)
- Virtual Private Networks (**VPNs**), private browsing and other anonymising tools
- Generative AI and synthetic media (**chatbots; image/video/voice generation; voice cloning/deepfakes**)
- Augmented and virtual reality (**AR/VR headsets, VRChat/Metaverse-style platforms**)
- Internet-connected smart devices (e.g. **smart speakers, wearables, trackers, IoT**)
- Anonymous Q&A and confession-style apps (e.g. **NGL, Tellonym**)
- Online marketplaces and payments, including in-app purchases, skins and loot boxes
- Music and media streaming services (e.g. **Spotify, Apple Music**) and podcast apps

Note: Brand names are illustrative only; access and use are governed by our Acceptable Use Policy, age-restrictions, and our filtering and monitoring standards.

How is Artificial Intelligence (AI) used safely and responsibly?

TASIS England recognises that artificial intelligence, including generative AI, can support teaching, learning, creativity and productivity when used appropriately. AI tools can also create safeguarding, privacy, accuracy and academic integrity risks. The School therefore expects all users to use AI safely, critically and responsibly.

- Students and faculty/staff must only use AI tools and platforms that are appropriate for their age, purpose and role and, where required, have been approved by the School.
- Personal, confidential, special-category or safeguarding information must not be entered into unauthorised AI tools. This includes information that could identify students, parents, faculty or staff.
- Students must follow their teachers' instructions about when AI may or may not be used for schoolwork. AI must not be used to cheat, plagiarise, impersonate another person or misrepresent work as entirely the student's own.
- Where AI has been used to support assessed work, students should acknowledge its use where required by the teacher, department, examination board or School academic-integrity procedures.
- Information produced by AI may be inaccurate, misleading, incomplete, biased or fabricated. Students and faculty/staff must critically evaluate and verify AI-generated information rather than assuming it is correct.
- AI-generated images, audio, video or other synthetic media must not be used to bully, harass, humiliate, threaten, deceive or impersonate another person.
- Creating, requesting, possessing or sharing AI-generated sexual or indecent images involving children is prohibited and will be treated as a safeguarding concern. This includes manipulated images, deepfakes and other synthetic sexual content.
- Students must not use AI systems to seek advice or engage in conversations that cause them concern or make them feel unsafe. Where an AI system produces harmful, sexual, violent, discriminatory, extremist or otherwise concerning content, students should stop the interaction and report it to a trusted adult.
- The School may apply filtering and monitoring arrangements to the use of AI services on School systems and devices in accordance with its safeguarding, Online Safety and data protection arrangements.
- Faculty/staff using AI remain professionally responsible for the accuracy, appropriateness and quality of any material they create or use. AI output must not replace professional judgement, safeguarding decision-making or appropriate human oversight.
- Any suspected misuse of AI will be addressed in accordance with the Online Safety Policy, Behaviour Management, Discipline and Sanctions Policy, Safeguarding Children and Child Protection Policy, Data Protection Policy and relevant Acceptable Use Policies.

How to react to misuse by students and young people:

- **Step 1:** Should it be considered that a child or young person has deliberately misused IT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.

- **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the Internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a senior administrator and the most appropriate course of action will be agreed.
- **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding Children Child Protection Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

How is printing managed? The use of the IT printers may be monitored on an individual basis to encourage careful use of printing resources. As well as being a significant capital cost, the consumables (ink, laser printer toner and drums, and paper) associated with printing represent one of the most expensive ongoing costs associated with IT. Whilst the school would not wish to discourage the proper use of printers, it is important to ensure that printing facilities are used efficiently and effectively. Students and staff are asked to take care not to waste printing resources, for example by using "Print Preview" to check work before sending it to the printer and by using colour print only when necessary.

What are the categories of cyberbullying? Seven categories of cyberbullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to students or young people or posting inappropriate material in a public digital locale.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where students and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

General housekeeping: The IT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition, the IT resource is finite e.g., computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes but will consider doing so should the need arise.

The following will apply:

- Treat IT equipment with respect and keep areas around IT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

What are the student rules?

- Do not use IT without permission.
- Food and drink must not be consumed near any computer equipment anywhere in the school.

- Do not move about the room while seated on a chair.
- Any person found defacing or wilfully damaging IT equipment will be required to correct the damage caused or pay for replacement.
- Computer faults should be promptly reported to the IT Manager. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at the workstation.
- At the end of a session:
    - Log off/shut down according to instructions.
    - Replace laptops as directed.
    - Wind up and put away any headsets.

What has research into cyberbullying found? Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyberbullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyberbullying is done by students in the same class or year group and although it leaves no visible scars, cyberbullying of all types can be extremely destructive.

- Between a fifth and a quarter of students have been cyber-bullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyberbullying.
- There is more cyberbullying outside school than in.
- Girls are more likely than boys to be involved in cyberbullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyberbullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyberbullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyberbullied tell no one about the bullying.

What is the impact on a child of IT based sexual abuse? The impact on a child of IT based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. IT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response are recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

How do I stay secure on the Internet?

- Do not type any personal details (including your name or email address) into a web site unless you are absolutely sure of the authenticity and trustworthiness of the associated company.
- The use of chat rooms is prohibited.
- The use of Instant Messaging is prohibited.
- The use of Internet-based email or newsgroups is prohibited except with the prior written approval of the Head.

Why is promoting safe use of IT important? TASIS England takes very seriously the importance of teaching students (and staff) to use IT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of IT in school, but also outside school in the wider community.

What does the school's mobile phone policy include?

- The commitment to keep the students safe.
- How we manage the use of mobile phones at TASIS England taking into consideration faculty, staff, students on placement, volunteers, other professionals, trustees, visitors and parents/carers.
- How we inform parents/carers, visitors and other professionals of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.

- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children and Child Protection Policies.

Prevent - top ten FAQs: Below are some of the most frequently asked questions received by the Independent Schools Inspectorate in relation to Prevent and inspections.

Where can we learn more about *Prevent*? There are two key source documents for the *Prevent* strategy:
- Statutory guidance (Home Office) - see paras 1-27 generally and 57-76 for sector specific guidance for schools
- Advice for schools (Department for Education)

What do we have to do? The overarching legal duty is to **"have due regard to the need to prevent people from being drawn into terrorism"** and, in so doing, have regard to guidance issued by the Secretary of State. In summary, the national statutory guidance from the Home Office, and sector-specific advice from the Department for Education places the following expectations on schools:
- **Demonstrate effective leadership:** display an awareness and understanding of the risk of radicalisation in your area and institution; communicate and promote the importance of the Prevent duty to staff; ensure staff implement the Prevent duty effectively.
- **Train faculty/staff:** ensure faculty/staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism; ensure faculty/staff have the knowledge and confidence to identify students at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism and are shared by terrorist groups; ensure staff know where and how to refer students and young people for further help.
- **Work in partnership with other agencies:** co-operate productively, in particular, with local Prevent coordinators, the police and local authorities, and existing multi-agency forums, for example Community Safety Partnerships; ensure that safeguarding arrangements consider the policies and procedures of the Surrey Safeguarding Children's Partnership (SSCP).
- **Share information appropriately:** ensure information is shared between organisations to ensure, for example, that people at risk of radicalisation receive appropriate support.
- **Risk assessment:** assess the risk of students being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This should be based on an understanding, shared with partners, of the potential risk in the local area or your school's particular circumstances. This means being able to demonstrate both a general understanding of the risks affecting students and young people in the area and a specific understanding of how to identify students who may be at risk and what to do to support them.
- **Build resilience to radicalisation:** promote fundamental British values through the curriculum and through social, moral, spiritual and cultural education; equip students with knowledge, skills and understanding to prepare them to play a full and active part in society; ensure your school is a safe place to discuss sensitive issues, while securing balanced presentation of views and avoiding political indoctrination.
- **Safeguard and promote the welfare of students:** put in place robust safeguarding policies to identify students at risk and intervene as appropriate by making referrals as necessary to Channel or Children's Social Care, for example.
- **Ensure suitability of visiting speakers:** operate clear protocols for ensuring that any visiting speakers, whether invited by staff or by students themselves, are suitable and appropriately supervised. See Safeguarding Child Protection Policy.

IT policies: ensure students are safe from terrorist and extremist material when accessing the Internet in school, including by ensuring suitable filtering is in place. The DfE advises that Internet safety will usually be integral to IT education and can also be embedded in PSHEE, for example. Every teacher needs to be aware of the risks posed by online activity of extremist and terrorist groups. It is for schools to use their own judgement to fill in operational detail about how best to implement the duty in the context of the level of risk in their locality as advised by their Surrey Safeguarding Children Partnership (SSCP) or other local agencies and the assessed risks to their own students. The role of inspectors is to raise awareness of the duty and consider whether the measures schools have in place appear effective in each school's particular context. In particular, inspectors will check that schools know how to respond to students who may be targeted or influenced to participate in radicalism or terrorism.

Do we have to have a separate *Prevent* policy? The Prevent duties can largely be implemented through schools' existing safeguarding duties using, for example, current reporting lines and training processes. It is not a requirement to create a separate dedicated *Prevent* Policy. However, the Home Office statutory guidance introduces a new requirement that policies "set out clear protocols for ensuring that any visiting speakers - whether invited by faculty, staff or by students themselves - are suitable and appropriately supervised." This protocol can be a standalone document or be part of another policy or document.

What IT filtering systems must we have? No technical guidance has been prescribed concerning the levels of filtering which are to be considered appropriate. This means that schools have discretion as to how they approach this aspect of the prevent duty. Inspectors will assess and challenge on the basis of whether what is in place appears effective in practice to ensure students are kept safe from terrorist and extremist material when accessing the Internet in school. Keeping safe online is as much about educating students to think critically and about appropriate behaviour online as technical solutions.

What is the definition of a visiting speaker? There is no definition of a visiting speaker. Schools should exercise their own reasonable judgement to determine who is a visiting speaker.

Do we have to check all our visiting speakers? Schools must ensure all visiting speakers are suitable. There is scope for local discretion as to how. For example, a school could choose to check all speakers or to check all those whose risk assessment indicates warrant closer attention. The overarching strategy should be recorded in the written protocol mentioned in 3 above. When it comes to inspection, the burden is on the school to demonstrate to inspectors how they meet the duty. Inspectors will expect verbal assurances from schools to be backed up by documentary and other evidence that protocols are put into practice on the ground.

What checks must we run on visiting speakers? Our safeguarding (Child Protection) Policy, in line with KCSIE (2026) sets out the arrangements for individuals coming onto the premises, which includes an assessment of the educational value, the age appropriateness of what is going to be delivered and whether relevant checks will be required. Schools need not confine their approach to the usual formal checks; Internet searches, for example, may sometimes be more instructive than formal vetting checks. The school will ensure that any information or content that a visiting speaker will present to staff or students is agreed beforehand, to check its suitability. The school will decide which formal checks are required, in accordance with regulatory compliance, as appropriate by reference to the usual considerations such as role, frequency, supervision, payment (as not all visiting speakers are volunteers), or whether speakers are employed by another organisation.

What training must we have? As a minimum, schools should ensure that the Designated Safeguarding Lead undertakes Prevent awareness training and is able to provide advice and support to other members of staff on protecting students from the risk of radicalisation. Schools should consider and arrange further training in the light of their assessment of risks.

What are the potential legal consequences if we do not take the *Prevent* duty seriously? Where the Secretary of State is satisfied that a school has failed to discharge the duty under the Prevent strategy to have regard to the need to prevent people from being drawn into terrorism, the Secretary of State may give directions to the school to enforce performance of the duty. A direction can be enforced by court order.

What are the rules for publishing content online?

- Faculty/staff or Student personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number.
- Student's full names will not be used anywhere on the school website or other online space.
- We may use photographs of students or their work when communicating with parents and the wider community, in newsletters and in the school prospectus.
- Photographs will be checked to ensure that they are suitable (photos of students in swimwear would be unsuitable).

Appendix 6: Parents, Volunteers and Visitors Photographing Students

TASIS England provides an environment in which students, parents and staff are safe from images being recorded and inappropriately used. The growth of hand-held mobile technology and interconnectivity has implications for the safety of students, so in order to reflect the policy on safeguarding and child protection, upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of students, or to take photographs of students apart from circumstances as outlined below. This includes where students are on school trips or residential. Neither are volunteers or visitors permitted to take photographs or recordings of the students. Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of students. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school.

Parental use of mobile phones/cameras whilst on the school grounds: TASIS England allows parents to take photos of their own children at organised events such as a school performance, sporting event or celebration of learning. We will remind audiences of this at the start of each event, where practicable. Faculty and staff will also remind parents regularly of school policy regarding mobile phone use with the following statement when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g., a family album) and so are exempt from the Data Protection Act 2018. Please be aware these images (which may include other students) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of the Act." If parents wish to make or take an emergency call whilst on school grounds, they may use the office and the school phone.

Parents are welcome to take photographs of their own students taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others. Flash photography can disturb others in the audience or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events. Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the program of events where issues of copyright apply. Additionally, the school records images of students, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph professionally events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of students while performing and disturbance within the audience.

When students join TASIS England, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld, this must be made clear when the consent form is returned to school so that photographs/videos are not published of the individual child concerned. The students take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents are welcome to take photographs of these memorable events, which may include groups of students. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents. Wherever possible, parents who take photographs of groups of children who are in the care of the school should gain consent first, ensuring that once any photographs are taken, they are stored safely and not posted to social media. The school recognises that it cannot police parents taking photographs of students who are outside school grounds and not in the school's care, however posting such pictures online may be in breach of the Data Protection Act 2018 without consent of all people within the photograph.

IMAGE RELEASE CONSENT FORM

TASIS England wishes to share photographs and videos of your child(ren) to:

- Celebrate their learning, service, and accomplishments, and
- Illustrate all that our school can offer to prospective students and families.

We never identify students by their full name. Any names used in text or captions would, at most, be first name and initial of surname only.

TASIS England can lawfully process and use such images, subject to receiving consent to do so. As indicated in our *Privacy Notice for Parents and Students* (see Appendix 1 of TASIS England's Data Protection Policy), the final decision regarding consent rests with you, as parents/carers. A child, if over the age of 13, may give or withdraw consent themselves. However, we are requesting **your** consent to use images of your child(ren) for the purposes described below.

If you choose to withhold consent, please discuss your wishes with your child(ren) so that they will understand why they must be excluded from group photos and videos. Your consent can be given or withdrawn at any time by emailing communications@tasisengland.org.

Internal Distribution

I give permission for my child(ren)'s image (photographs and/or video) to be used:

- In school publications, such as yearbooks, class or team photographs, theatre and concert programs, etc.
- In and around the school, including on bulletin boards, displays, and information screens that may be viewed by classmates, teachers, and visitors to the school; and
- In communications to members of the school community, such as newsletters to parents, faculty, staff, and alumni.

☐ Agree

☐ Disagree

External Distribution

I give permission for my child(ren)'s image (photographs and/or video) to be used for the school's wider marketing and promotional purposes such as:

- in the prospectus, brochures, parent handbooks, etc.;
- on the website;
- on the social media channels;
- in newsletters to prospective families and TASIS England partners (e.g., education consultants);
- In advertising (print and digital); and
- other such external-facing communications and publications.

☐ Agree

☐ Disagree

Acceptable Use of Mobile Phones and 3G/4G/5G compatible devices - Whole School

It is our intention to provide within this policy an environment in which children, parents, and staff are safe from images being recorded and inappropriately used, in turn eliminating the potential use to interfere with the dignity and privacy of all individuals and thus compromise the confidentiality of the children in our care.

Purpose:

- The widespread ownership of mobile phones and 3G/4G/5G compatible devices (referred to throughout this document as mobile devices) among young people requires that school administrators, teachers, students, parents and carers take steps to ensure that these devices are used safely and responsibly at school. This Acceptable Use Policy is designed to ensure that potential issues involving mobile devices can be clearly identified and addressed, ensuring the benefits that they can provide can continue to be enjoyed by our students.
- TASIS England has established the following Acceptable Use Policy for mobile devices that provides teachers, students, parents and carers guidelines and instructions for the appropriate use of these devices during the time students are under the care of TASIS England, inclusive of the academic day, the boarding program, on campus and all educational visits.
- Students, their parents or carers must read and understand the Acceptable Use Policy as a condition upon which permission is given to bring mobile devices to school.

Rationale:

- The school recognises that personal communication through mobile devices such as mobile technologies is an accepted part of everyday life, therefore such technologies are to be used responsibly and in accordance with the TASIS England Acceptable Use Policy.
- TASIS England accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can make contact with their child if they need to speak to them (in accordance with the TASIS England Mobile Phone Policy).

Responsibility:

- It is the responsibility of students who bring mobile devices to school to follow the guidelines outlined in this document, particularly Appendix 7.
- The decision to provide any mobile devices to their children should be made by parents or carers. It is important that parents understand the capabilities of these devices and the potential uses or misuses of those capabilities. If needed, guidance to this information can be signposted by the school.
- Parents/carers should be aware that if their child brings any device, including a mobile phone to school, the school does not accept responsibility for any loss, damage or costs.
- Parents/carers are reminded that in cases of emergency, the school remains a vital and appropriate point of contact and can ensure your child is reached in a relevant and appropriate way. Parents/carers are requested that in cases of emergency they contact the school first so we are aware of any potential issue and may make any necessary arrangements.

Acceptable Uses:

- Mobile phones should be switched off and kept out of sight during classroom lessons and the regular school day in order to minimize disruption or distraction.
- Mobile phones should not be used in any manner or place that could be disruptive to the normal routine of the school.
- Headphones/earphones should only be used during private study or travelling to and from school with permission from the teacher.

Unacceptable Uses:

- In order to protect one's privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, surf the internet, take photos or use any other application during the school day including educational activities such as assemblies, study halls, or in the TASIS England Dining Halls.

- Mobile devices should not disrupt the school day with ring tones, music or beeping. They should be turned off during the school day in order to respect the learning environment. Using mobile phones to bully and threaten other students is unacceptable. Cyberbullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. (Please refer to the Anti-bullying and Online Safety and IT Policies.)
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.
- Disruption to the school day caused by a mobile phone or any mobile device may lead to disciplinary consequences as outlined in the mobile phone policy (Appendix 7 below) and the student Behaviour Management policy.
- Safeguarding, privacy and respect are paramount at TASIS England. To this end, it is prohibited to take a picture of or record a member of staff without their permission. If this happens the student will be asked and expected to delete those images and will turn over the device to the Head of School and/or the TASIS England Designated Safeguarding Lead.
- For safety reasons, headphones/earphones should not be used whilst moving around campus during the school day, whilst waiting for or during lessons and assemblies, or in the TASIS England dining halls.

Theft or damage:

- Mobile phones or any mobile devices that are found in the school and whose owner cannot be located should be handed to the front office reception or TASIS England Security.
- The school accepts no responsibility for replacing lost, stolen or damaged devices.
- The school accepts no responsibility for damage to or loss of mobile phones or mobile devices while travelling to and from school.
- It is strongly advised that students use passwords/pin numbers to ensure that unauthorized phone calls cannot be made on their phones or other mobile devices. Students must keep their password/pin numbers confidential.

Inappropriate conduct:

- Under exam regulations, mobile phones are prohibited from all examinations. Students MUST give phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.
- Any student who, at any time, uses vulgar, derogatory, or obscene language while using a mobile phone may face disciplinary action.
- Academic Study Hall time is an extremely important part of the TASIS England education. In order to ensure all boarders study time is respected, boarding students must not use their mobile phones or mobile devices during evening study hall hours unless explicitly required by their teacher for a specific assignment.
- TASIS England values the health and wellbeing of every student. To this end, boarding students must not use their mobile phones or mobile devices after evening checks are made in the Houses or after evening "lights out".
- Students with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using messages, taking/sending photos or objectionable images, and phone calls. Students using mobile phones, at any time, to bully other students will face disciplinary action. (It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, the school may consider it appropriate to involve the police). Please refer to our Online Safety and the Upper School Behaviour Guidelines for further information.
- Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence, and the school is obliged to report any findings of this nature to the police and local authority.
- Similarly, sending nude or semi-nude images is also a criminal offence, which obliges the school to report to the police and local authority.

Measures: The following measures may be used in consultation and conjunction with the Anti-bullying , Safeguarding Children and Child Protection and, Online Safety and IT Policies. The TASIS England DSL and Online Safety Coordinator must be consulted when inappropriate conduct requires a mobile phone to be confiscated and searched.

- Students who violate the rules set out in this document could face having their phones and/or mobile devices held by teachers, House Parents, Deputy House Parents or House Tutors until the end of the school day or study hall session. If the device is being used inappropriately the student must give it to the supervising adult if requested.
- Violation of the rules set out in this document are subject to the disciplinary measures and sanctions set out in Appendix 7 of this policy and the TASIS England Behaviour Management, Discipline & Sanctions Policy, which can be found on the policy section of the TASIS England Website.

I have read and understand this policy:

Student signature: _____ Parents: Informed via email communication

Appendix 7: Grades 5-8 and Upper School Student Mobile Phone Policy

1. Introduction and aims

In alignment with the UK government's guidance on safeguarding and promoting the welfare of children, this policy outlines the School's commitment to protecting students' mental health concerning the use of mobile phones and mobile phone technology. Recognizing the serious impact of mobile phone use on students' learning and mental health, TASIS England aims to create a safe and supportive environment that minimises distractions to learning, promotes wellbeing, and encourages healthy habits around technology use.

The UK Department for Education states that all schools should be mobile phone-free environments by default and that students should not have access to their mobile phones throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime (Mobile phones in schools, DfE statutory guidance, to be followed from 1 September 2026).

At TASIS England we recognise that mobile phones and similar devices are an important part of everyday life for our students and wider school community, and we aim to set clear guidelines for the use of mobile phones in school, while also promoting safe and responsible use of mobile phone technology in our students' lives.

Note: throughout this policy, 'mobile phones' refers to mobile phones as well as any similar devices.

2. Relevant guidance

This policy meets the requirements of the Department for Education's Mobile phones in schools' statutory guidance, to be followed from 1 September 2026, and Behaviour in Schools guidance (DfE 2024).and behaviour guidance (DfE 2024). Further guidance that should be considered alongside this policy is Keeping Children Safe in Education (DfE 2026). The DfE's Mobile phones in schools' statutory guidance states that all schools should be mobile phone-free environments by default, with anything other than this by exception only, and applies equally to other smart technology with similar functionality, such as smart watches. This expectation is reflected in the Independent School Standards guidance (April 2026, paragraphs 3.21-3.23) and, for state-funded schools, is placed on a statutory footing by section 36 of the Children's Wellbeing and Schools Act 2026 (in force 29 June 2026).

3. Roles and responsibilities

All faculty and staff (including teachers, support staff and volunteers) are responsible for consistently enforcing this policy. This policy is reviewed and maintained by Section Heads.

4. Use of mobile phones by students

- Students may not use or access mobile phones on campus, which includes (but is not limited to) arrival and departure times, lesson times, passing time between lessons, bathroom breaks, lunch times, study halls, or free study periods. Students in Grades 5-10 must comply with the relevant Section's arrangements for handing in and/or secure storage of mobile phones. Students in Grades 11-12 may retain possession of their mobile phones, but devices must remain switched off and securely stored and may not be used or accessed during the school day.

- Students may not use mobile phones during co-curricular activities.

- Students may not use mobile phones on field trips or during school-related travel without the permission of the trip leader or chaperones.

- Boarding students must hand their mobile phones in to their House Parents before school and may collect them after school/activities each day.

- Boarding students in Grades 8-10 must hand their mobile phones in to their House Parents overnight on Sunday-Thursday. Boarding students in Grades 11-12 will have the option of handing in their phones to be stored overnight on Sunday-Thursday.

- Where the parents of day students wish to send their child(ren) to school with a mobile phone or similar device for use during travel to and from school only, the device must be switched off on arrival and may not be used or accessed at any point during the school day. It must be stored in line with the sectional arrangements until departure.

- Students may not access mobile phone technology on any other device during the academic day or during co-curricular activities. These may include, but are not limited to, iPads, tablets, laptops, ear pods, or smart watches.

Emergencies or Necessary Communication Home:

- When communication between students and their parents is required during the academic day, students can make calls in private from the relevant sectional office. School staff will assist any student needing to call home.

- Parents needing to contact their children during the academic day should call the relevant sectional office. Information that is not time-sensitive should be shared through email.

- In exceptional circumstances, such as those related to documented medical needs, a student may receive special permission to have their mobile phone visibly with them during the academic day. Parents should contact the school in these circumstances to make the necessary arrangements.

5. Sanctions

- If a mobile phone is visible during the academic day, the student will receive a behavioural notification resulting in a detention.

- Faculty and staff may confiscate any mobile phones that are visible during the academic day. During class, these would be confiscated in a phone box or bag for the duration of the lesson. During lunchtimes or study hall times, these may be confiscated in a centralised location.

- Failure to surrender a mobile phone for confiscation will be treated as a disciplinary matter.

- Multiple mobile phone infractions may result in the need to hand in devices daily to the relevant sectional school office for a determined period of time, along with daily check-ins outside of class time with a member of staff.

- Failure to show improvement after multiple mobile phone use infractions will result in a Behavioural Reflection Meeting (BRM) with the Head of Section and Director of Pastoral Care, which may lead to a Saturday detention, internal discipline day, or external suspension (fixed-term exclusion).

- Use of mobile phones or mobile phone technology to engage in any behaviours that impact on the learning or wellbeing of others will be treated as separate disciplinary issues and carry separate consequences, in addition to those related to ordinary mobile phone use in school.

In addition, certain types of conduct, bullying or harassment can be classified as criminal conduct. See the school's Behaviour policy for more information.

6. Loss, theft or damage

Students bringing mobile phones to school for use during their commute to and from home must ensure that their phones are appropriately labelled and are stored securely at the bottom of their school bag at all times.

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while students are travelling to and from school.

If there are any concerns regarding this policy, please raise them with the relevant Section Head.