WELLINGTON COLLEGE
INTERNATIONAL SCHOOL BANGKOK

E-safety (Acceptable Use) Policy

Approval:	Executive Board	**Level:**	Public
Writer:	Bursar	**Review Frequency:**	2-Yearly
Next Review:	May 2027	**This Policy Approval:**	May 2025
Linked Policies:	Data Protection Policy; Record Keeping Policy; Disciplinary Policy (Staff); Staff Code of Conduct; Anti-bullying Policy; Behaviour Policy; Passwords Procedures; Child Protection & Safeguarding; Taking, Storing and Using Pictures of Children Policy.		

1. Introduction

1.1. Wellington College International School Bangkok ('WCIB' or 'the School') aims to:

1.1.1. Have robust processes in place to ensure the online safety of students, staff, volunteers, and governors.

1.1.2. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

1.1.3. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

2.1. This Policy is based on the UK Department for Education's safeguarding guidance, *Keeping Children Safe in Education*, and its advice for schools on preventing and tackling cyber-bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

2.2. The Policy generally reflects UK legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which allows teachers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices, when they believe there is a 'good reason' to do so.

2.3. The policy takes into account the National Curriculum Computing programmes of study.

2.4. This Policy also considers Thai legislation relevant to data protection (Personal Data Protection Act, B.E. 2562) and child protection laws applicable in international school contexts.

3. Roles and responsibilities

3.1. The **WCIB Board**

3.1.1. The WCIB Board has overall responsibility for monitoring this Policy and holding the Master to account for its implementation.

3.1.2. The WCIB Board will discuss online safety with the Senior Leadership Team, and review reports and data provided by the Designated Safeguarding Lead (DSL).

3.1.3. A WCIB governor will be nominated to oversee online safety as part of their responsibility as the governor lead for Safeguarding and Child Protection.

3.1.4. All governors will:

3.1.4.1. Ensure that they have read and understand this Policy.

3.1.4.2. Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2).

3.2. The **Master**

3.2.1. The Master is responsible for ensuring that all staff understand this Policy, and that it is being implemented consistently throughout the School.

3.3. The **DSL** takes lead responsibility for online safety in the School, in particular:

3.3.1. Supporting the Master in ensuring that staff understand this Policy and that it is being implemented consistently throughout the School.

3.3.2. Working with the Master, Bursar, Head of IT and other staff, as necessary, to address any online safety issues or incidents.

3.3.3. Ensuring that any online safety incidents are logged through CPOMS and dealt with appropriately in line with this Policy.

3.3.4. Ensuring that any incidents of cyber-bullying are logged through CPOMS and dealt with appropriately in line with the WCIB Behaviour Policy.

3.3.5. Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs).

3.3.6. Liaising with other agencies and/or external services as necessary.

3.3.7. Providing regular reports on online safety in school to the Master and/or Executive Board.

3.3.8. This list is not intended to be exhaustive.

3.4. The **Bursar**, as the School's Data Protection Officer, is responsible for:

3.4.1 Ensuring that this Policy is compliant with the WCIB Data Protection Policy and Record Keeping Policy.

3.4.1 Ensuring that all staff comply with the requirements under the Personal Data Protection Act ('PDPA') that all Personal Data is collected, recorded, stored and destroyed in a safe manner.

3.5. The **Head of IT,** is responsible for:

3.5.1. Implementing and maintaining appropriate filtering and monitoring systems, including those applied to the school's firewall, school-owned iPads, laptops, and other devices to ensure students are protected from potentially harmful or inappropriate content and contact online while at the School, including terrorist and extremist material.

3.5.2. Ensuring that the school's IT infrastructure are secure and protected against viruses, malware, phishing and other cyber threats. Safety mechanisms and software must be reviewed and updated regularly. Conducting and documenting regular IT system audits and security checks, and maintaining an active program of monitoring across the network to detect unusual activity or potential breaches. Supporting the implementation of the School's BYOD Policy for Sixth form students by ensuring appropriate network level controls, security monitoring, and device access restrictions are in place. This includes ensuring BYOD devices comply with minimum security standards and monitoring protocols while connected to the WCIB network.

3.5.3. Responding quickly and effectively to any security incidents or data breaches, including identifying the cause of the incident, mitigating further risks, and reporting in line with the school's data protection policy and legal obligations. Blocking access to unsafe or age-inappropriate websites and platforms, and where applicable, restricting downloads that pose a security risk or contravene the school's Acceptable Use Policy (AUP). Ensuring that any online safety incidents are logged and dealt with appropriately in line with this Policy.

3.5.4. Ensuring that any incidents of cyber-bullying are raised with academic staff.

3.5.5. Keeping up to date with technological advancements, digital safeguarding risks, and government guidance on e-safety, and applying this knowledge to school practice and policy updates.

3.5.6. Collaborating with the DSL, SLT, and academic staff to ensure a whole-school approach to online safety, digital citizenship education, and the promotion of safe and responsible use of technology.

3.5.7. Supporting the delivery of staff training on IT security, data protection, and e-safety, ensuring all staff are aware of their roles and responsibilities. .

3.5.8. This list is not intended to be exhaustive.

3.6. **All staff** including contractors and agency staff, and volunteers are responsible for:

3.6.1. Reading and understanding this Policy.

3.6.2. Implementing this Policy consistently.

3.6.3. Agreeing and adhering to the terms on acceptable use of the School's IT systems and the internet (appendix 2), and ensuring that students follow the School's terms on acceptable use (appendix 1).

3.6.4. Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this Policy.
3.6.5. Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the WCIB Behaviour Policy
3.6.6. This list is not intended to be exhaustive.

3.7. **Parents** are requested to:
3.7.1. Notify a member of staff or the Master of any concerns or queries regarding this Policy.
3.7.2. Ensure their children have read, understood, and agreed to the terms on acceptable use of the School's IT systems and internet (appendix 1).
3.7.3. Parents can seek further guidance on keeping children safe online from the following organisations and websites:
3.7.3.1. What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
3.7.3.2. Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

3.8. 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 expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating students about online safety

4.1. Students are taught about online safety as part of the curriculum.
4.2. In Years 1-2, students are taught to:
4.2.1. Use technology safely and respectfully, keeping personal information private.
4.2.2. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
4.3. In Years 3-6, students are taught to:
4.3.1. Use technology safely, respectfully, and responsibly.
4.3.2. Recognise acceptable and unacceptable behaviour.
4.3.3. Identify a range of ways to report concerns about content and contact.
4.4. In Years 7-9, students are taught to:
4.4.1. Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
4.4.2. Recognise inappropriate content, contact, and conduct, and know how to report concerns.
4.5. In Years 10-11, students are taught:
4.5.1. To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.

4.5.2. How to report a range of concerns.

4.6. The safe use of social media and the internet are also covered in other subjects where relevant.

4.7. The School uses assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

5.1. The School raises parents' awareness of internet safety in letters or other communications home, and in information via our website and/or parent portal. This Policy is also shared with parents.

5.2. Online safety is also covered during parents' workshops.

5.3. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Master and/or the DSL.

5.4. Concerns or queries about this Policy can be raised with any member of staff or the Master.

6. Cyber-bullying

6.1. Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the WCIB Behaviour Policy.)

6.2. Preventing and addressing cyber-bullying:

6.2.1. We ensure that students understand what it is, and what to do if they become aware of it happening to them or others.

6.2.2. We ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

6.2.3. The School actively discusses cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers, Tutors and Heads of House discuss cyber-bullying with their groups, and the issue is addressed in assemblies.

6.2.4. Aspects of the curriculum are also used to cover cyber-bullying as appropriate. This includes Wellbeing education.

6.2.5. All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

6.2.6. The School may also send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

6.2.7. In relation to a specific incident of cyber-bullying, the School will follow the processes set out in the WCIB Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, the School will use all reasonable endeavours to ensure the incident is contained.

6.2.8. The DSL, in consultation with the Master and, where appropriate, the Head of IT, will consider whether an incident should be reported to the police and will work with external services if it is deemed necessary to do so.

6.3. Examining electronic devices

6.3.1. School staff may search for and, if necessary, request to delete inappropriate images or files on students' personal electronic devices, including mobile phones, iPads, and other tablet devices, where the Master believes there is a 'good reason' to do so. Students are required to allow full access to all areas of a personal device, including password-protected areas, in such cases.

6.3.2. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

6.3.2.1. Cause harm, and/or

6.3.2.2. Disrupt teaching, and/or

6.3.2.3. Break any of the School rules.

6.3.3. If inappropriate material is found on the device, it is up to the DSL in consultation with the Master to decide whether they should:

6.3.3.1. Delete that material, or

6.3.3.2. Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

6.3.3.3. Report it to the police.

6.3.4. Any searching of students' devices will be carried out with consideration of the UK DfE's latest guidance on screening, searching and confiscation, and in accordance with Thai law.

6.4. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the WCIB Complaints Procedures.

7. Acceptable use of the internet and 4G/5G in school

7.1. All students, parents, staff, volunteers, and governors are bound by the rules regarding the acceptable use of the School's IT systems and the internet (Appendices 1 and 2). Visitors are expected to read and abide by the School's rules on acceptable use.

7.2. Use of the School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

7.3. The School monitors the websites visited by students, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

7.4. The use of any personal device on the School premises through a 4G or 5G connection by any student, parent, staff member, volunteer, governor, or visitor must comply with the same high expectations for acceptable use that regulate the use of devices on the School's internet. Accessing inappropriate material on the School premises may lead to sanctions or disciplinary action.

7.5. More information is set out in the Acceptable Use Rules in Appendices 1 and 2.

8. Students using mobile devices in school

8.1. Students in Year 4 and above may bring mobile devices into School, but are not permitted to use them at all during school hours.

8.2. Sixth Form students are permitted to bring their own devices under the WCIB BYOD Policy. This Policy has been signed by both students and parents and outlines acceptable use, network access, and security expectations. BYOD devices are subject to the same e-safety, filtering, and monitoring requirements as school-owned devices when connected to the School's network.

8.3. Any Student-owned device will be securely locked away during school hours and may be reclaimed at the end of the day. Smart watches and any similar devices that have wireless communication functions enabled are considered to be mobile devices under this rule.

8.4. Any breach of the acceptable use rules by a student may trigger disciplinary action in line with the WCIB Behaviour Policy.

9. Staff using work devices outside school

9.1. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's rules for acceptable use, as set out in Appendix 2.

9.2. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others in line with the WCIB Password Procedures. They must take all reasonable steps to ensure the security of their work device when using it outside school.

9.3. No USB devices may be used on the School premises and through the School's devices without prior written approval from the Bursar.

9.4. If staff have any concerns over the security of their device, they must seek advice from the Head of IT.

9.5. Work devices must be used solely for work activities.

10. How the School responds to issues of misuse

10.1. Where a student misuses the School's IT systems or internet, the School follows the procedures set out in the WCIB Behaviour Policy. The action taken depends on the

individual circumstances, nature' and seriousness of the specific incident, and is proportionate.

10.2. Where a staff member misuses the School's IT systems or internet, or misuses a personal device and the action constitutes misconduct, the matter is dealt with in accordance with staff Disciplinary Policy and Procedures. The action taken depends on the individual circumstances, nature, and seriousness of the specific incident.

10.3. Where incidents involve illegal activity or content, or otherwise serious incidents, the School will make a report to the police.

11. Training

11.1. All new staff members receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

11.2. All staff members receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through CPD sessions, emails, bulletins, and staff meetings).

11.3. The DSL undertakes child protection and safeguarding training, which includes online safety, at least every 2 years. They also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

11.4. Governors receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

11.5. Volunteers receive appropriate training and updates, if applicable.

11.6. More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring arrangements

12.1. The DSL logs behaviour and safeguarding issues related to online safety.

12.2. This Policy is reviewed every two years by the Senior Leadership Team. At every review, this Policy is shared with the Executive Board.

12.3. The Head of IT will provide technical updates and reports on filtering, monitoring, and security to the DSL and SLT on a regular basis, in support of safeguarding reporting.

13. Acceptable Use for Remote Learning

13.1. Remote learning only takes place via Seesaw, Zoom or MS Teams.

13.2. Staff may only use WCIB's managed, approved, professional accounts with students and parents.

13.3. Use of any personal accounts to communicate with students and/or parents is not permitted.

13.4. Any pre-existing relationships or situations which mean the above cannot be complied with must be discussed with the Designated Safeguarding Lead (DSL).

13.5. Staff use school-provided equipment wherever possible, for example their school laptop or iPad.

13.6. All remote lessons are formally timetabled, and all Teams and Zoom links made available on MS Teams; a member of SLT is permitted, and able, to drop in at any time if required or as appropriate.

13.7. Any personal data used by staff and captured by any of the Remote Learning systems when delivering remote learning are processed and stored with appropriate consent and in accordance with the School's Data Protection Policy.

13.8. All students and families are made aware that the School records all Teams and Zoom lessons. Recordings are retained securely in accordance with the School's Data Protection Policy and are only accessible to authorised WCIB staff.

13.9. Only members of the WCIB community may be given access to the School's Seesaw and Microsoft Accounts.

13.10. Students are encouraged to report concerns which may arise during Remote Learning to their Class Teachers or House Tutors, or a parent, who should then contact the School on their behalf.

13.11. If inappropriate language or behaviour takes place, participants involved will be removed from the Teams or Zoom session by staff, the session may be terminated, and concerns will be reported to a member of the SLT.

13.12. Sanctions for deliberate misuse may include:

13.12.1. Restricting or removing use

13.12.2. Contacting the police if a criminal offence has been committed.

14. Appendix 1: Acceptable Use Rules (for students)

14.1. When using the School's IT systems and/or accessing the internet in School on any device, students may not:

14.1.1. Use them for a non-educational purpose

14.1.2. Use them without a teacher being present, or without a teacher's permission

14.1.3. Access any inappropriate websites

14.1.4. Access social networking sites (unless a teacher has expressly allowed this as part of a learning activity)

14.1.5. Use chat rooms or other chat functions or environments

14.1.6. Open any attachments, or follow any links, without first checking with a teacher

14.1.7. Use any inappropriate language when communicating online, including in emails

14.1.8. Share passwords with others or log in to the School's network using someone else's details

14.1.9. Give personal information (including name, address, or telephone number) to anyone without the permission of a teacher or parent/carer

14.1.10. Arrange to meet anyone offline without first consulting a parent/carer, or without adult supervision

14.2. Regarding personal mobile phones and/or other personal electronic devices including smart watches while on campus or involved in a School activity, students may not:

14.2.1. Use them without a teacher's permission

14.2.2. If permitted to use them, do so irresponsibly, or access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

14.2.3. Take any photos, or make any video recordings, of any kind

14.3. The School may monitor any online activity and the Master is allowed complete access to any and all areas of any device a student is using whilst at School or engaged in a School event or activity, should he have reason to request it.

14.4. A Student must immediately let a teacher or other member of staff know if they find any material which might upset, distress or harm them or others.

14.5. Students must always use all IT systems and the internet responsibly.

Note: these rules form part of the rules of the School, by which all families and Students have already agreed to abide.

15. Appendix 2: Acceptable Use Rules (for staff, governors, volunteers, and visitors)

15.1. When using the School's IT systems and accessing the internet in School, or outside School on a work device, staff members must not:

15.1.1. Access, or attempt to access, inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature

15.1.2. Use them in any way which could harm the School's reputation

15.1.3. Social media access is prohibited unless specifically required for teaching or school communications. Use any improper or inappropriate language when communicating online, including in emails or other messaging services

15.1.4. Install any unauthorised hardware, software, or apps

15.1.5. Share any password with others or log in to the School's network using someone else's details

15.2. When using the School's IT systems and accessing the internet in School, or outside School on a work device, adults must only use them for educational purposes or for the purpose of fulfilling the duties of a specific role.

15.3. The School may monitor staff online activity, including websites visited.

15.4. Staff must take all reasonable steps to ensure that work devices are secure and password-protected when they are used outside School, and keep all data securely stored in accordance with this policy and the WCIB Data Protection Policy.

15.5. Adults must let the Designated Safeguarding Lead (DSL) and Head of IT know if a student informs them, they have found any material which might upset, distress or harm them or others, and must also do so if they encounter any such material.

15.6. All adults must always use the School's IT systems and internet responsibly and ensure that students in their care do so too.

16. Appendix 3: online safety training needs – self-audit for staff

Name of staff member/volunteer:

Date:

16.1. Do you know the name of the person who has lead responsibility for online safety in school?

16.2. Do you know what you must do if a student approaches you with a concern or issue?

16.3. Are you familiar with the School's Acceptable Use Rules for staff, volunteers, governors, and visitors?

16.4. Are you familiar with the School's Acceptable Use Rules for students?

16.5. Do you change your password for accessing the School's IT systems on an annual basis?

16.6. Are you familiar with the School's policy on cyber-bullying?

16.7. Are there any areas of online safety in which you would like training/further training? Please record them here.

17. Appendix 4: Social Media and photography/recording

17.1. For reasons of Child Protection and Safeguarding, members of the School, including parents and staff, may not

17.1.1. Take photos or make any type of recording, including video, on the School campus and/or during School events unless specifically permitted to do so by the Master.

17.1.2. School staff may not use personal devices for these purposes.

17.1.3. School marketing staff using school managed social media accounts are exempt if done under policy and with training.

17.1.4. Share or otherwise upload any images taken or made on the School campus and/or during School events to any social media or similar sites unless specifically permitted to do so by the Master.

17.2. School Staff must not 'friend' or otherwise connect with on public social media either students or their parents.

17.2.1. Staff who are also parents are not included in 17.2 in respect of social media links with other parents (not students); nevertheless, such staff should remain fully aware of their professional responsibilities as explored in this document.

17.3. School staff may not 'friend' or otherwise connect with on social media a student who has left the School until a period of at least two years has elapsed from the time that student was taken off the School roll, or the child is of school-leaving age, whichever is later.

17.4. School staff may not make specific comment on the School in their personal social media.

17.5. School staff are required to maintain appropriate levels of privacy in all their social media and similar activity, such that the good name of the School is never questioned or brought into disrepute as a result of any content, whether current or historical.