



# RUGBY SCHOOL THAILAND



## DIGITAL AWARENESS POLICY

THE WHOLE PERSON THE WHOLE POINT

*The health, safety and well-being of young people are of paramount importance to all the adults who work at Rugby School Thailand. Children have the right to protection, regardless of age, gender, race, culture, sexual orientation, or disability. They have a right to be safe in our school. Members of staff in the school have a legal and moral obligation to safeguard and promote the welfare of the students, taking all reasonable steps to protect them from harm whether from physical injury, abuse, neglect, emotional harm or from anything that interferes with their general development.*

#### Version Control

<b>Policy number:</b> RST_007	<b>Version number:</b> 2	<b>Effective Date:</b> 30 <sup>th</sup> November 2023
<b>Responsible:</b> Richard Burkhill	<b>Reviewed by:</b> Digital Wellbeing Team	<b>Date last reviewed:</b> 18 <sup>th</sup> November 2023
<b>Approved by Sub-Committee:</b> Finance Committee	<b>Approval Date:</b> November 2023	<b>Date of next review:</b> August 2024

<b>This policy relates to:</b>	Child Protection & Safeguarding Policy Code of Conduct Policy Terms & Conditions of Enrolment Staff Handbook
<b>Responsible Department(s):</b>	Richard Burkhill: Director of Digital Learning, Whole School Paul Corr: Director of Admissions & Marketing Dao Jitkasemsopon: Marketing Manager Oonagh Stoker: Marketing Coordinator / Social Media Manager Eric Ho: Director of I.T. Dave Ennis-Billing: Designated Safeguarding Lead
<b>Other standards:</b>	
<b>Legislation or other requirements:</b>	We are guided by UK and Thai legislative acts on copyright, data protection and Freedom of Information legislation. These include the Safeguarding Vulnerable Groups Act 2006 (UK), the Malicious Communications Act 1988 (UK), Child Protection Act 2003 (Thailand), PDPA 2020 (Thailand) and other legislation.

#### Review process

<b>Policy review frequency:</b> Annually	<b>Responsibility for review:</b> Director of Digital Learning
<b>Review process:</b>	
<ol style="list-style-type: none"> <li>I. Digital Wellbeing Team policy review (inc Director of Digital Wellbeing, DSL Whole School, DSL Senior, Deputy Head Pastoral &amp; DSL Prep, Deputy Head Pastoral Pre-Prep, Director of I.T. and Levee member)</li> <li>II. Modification will be made where appropriate</li> <li>III. Submit for review and approval by the Governors' Finance Committee</li> </ol>	
<b>Documentation and communication:</b>	

Document decision changes will be written in as addition and approved via SLT. There will be an update on the Version Number of the Document.

## Table of Contents

1. INTRODUCTION	5
2. POLICY AIMS	6
3. IMAGES	6
Privacy	6
Promotional Material	6
Taking of Images by Parents & Friends	7
Seeking Consent	7
Photographs as Part of Student Records	8
Use of Cameras, Video Cameras & Mobile Electronic Devices with Camera Facility	8
Child Protection	8
Taking of Images of Students by Staff	8
Recording Images of Students & Staff	9
4. SOCIAL MEDIA	10
Understanding Social Media	10
Guidance on Use of Social Media	10
Prohibited Use of Social Media	12
Safeguarding Policy Compliance	13
Use of Personal Devices	14
Primary & Secondary Social Media Accounts	14
School Trips or Excursions	15
Privacy & Security Settings	15
Monitoring	15
5. STUDENT ACCEPTABLE USE	16
6. STAFF ACCEPTABLE USE	17
Access	17
Computer Security & Data Protection	18
Use of Staff Owned Equipment	18
Conduct	19
E-Safety	19
Use of E-Mail	20

Use of Video Conferencing	21
Privacy	21
Confidentiality & Copyright	22
Reporting Problems with the Computer System	22
7. ONLINE SAFETY	22
8. BREACHES OF POLICY	23
9. APPENDICES	23

## 1. INTRODUCTION

- 1.1. This policy is addressed to all members of staff and available to parents and students. The policy relates to the use of photography, social media and acceptable usage of digital devices.
- 1.2. It covers the activities of staff, students, parents, and visitors to the School.
- 1.3. **Images:** this expression in relation to students includes:
  - photographs and digital photographs;
  - video or film clips;
  - images captured by mobile phones or other electronic devices.
- 1.4. **Taking images:** This expression includes, unless otherwise stated, making, editing, using, exhibiting, and storing images of students.
- 1.5. The widespread availability and use of social media applications such as Facebook, Instagram and Twitter, bring opportunities to market, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation.
- 1.6. The use of technology has become a significant component of safeguarding. Technology can provide a platform that facilitates harm, such as cyber-bullying, child sexual exploitation, radicalisation and sexual predation. An effective approach to online safety and social media usage can safeguard the children in our care, protect and educate the whole school community and empower them in their use of technology. It can also establish systems to identify, intervene with, and escalate any incident where appropriate.
- 1.7. With the spread of telecommunications through the modern workplace, the school recognises that staff may shift the way they share ideas, transmit information and contact others. Staff members are connected to the global community and the use of new tools and systems brings new responsibilities and opportunities.
- 1.8. It is important to safeguard staff and the School from abuse of the system. All staff, therefore, must adhere to the policy set out below and take responsibility for their own use of technologies, ensuring that they use this technology safely, responsibly and legally.
- 1.9. This policy covers all computers, laptops and electronic devices within the school, irrespective of who owns the device.
- 1.10. It is unlikely that any policy can cover all circumstances that may arise. The following policy is not intended to be a complete list of all possible “offences”. The emphasis is on outlining standards of performance and behaviour which are expected of our staff and students, when accessing the IT services of the School.
- 1.11. There are many issues classified within online safety, with three main areas of risk:
  - Content: being exposed to illegal, inappropriate or harmful material.
  - Contact: being subjected to harmful online interaction with other users.
  - Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

## 2. POLICY AIMS

2.1. The aims of this policy are to:

- promote safety and welfare and respect for others;
- ensure a sensible balance between privacy, creative self-expression, and routine collating of information;
- comply with the law and good practice without adhering to unnecessary bureaucratic procedures
- avoid the risks of using social media – both on official School channels and for personal use (especially with regards to showing School-related content)
- set professional boundaries in all forms of social media communication, to maintain public trust and appropriate professional relationships
- keep staff and students safe while utilising the IT equipment and services when in School
- enable staff to use IT equipment safely and effectively in order to support teaching and learning
- uphold high standards and provide guidance for the professional use of IT
- maintain the efficient application of the IT network and all IT equipment around the School.

## 3. IMAGES

### Privacy

3.1. No person is authorised to take images of children that:

- might cause embarrassment or distress; or
- are associated with distressing or sensitive issues; or
- are unnecessarily intrusive.

3.2. Filming and photography by any third party not employed by the School, including media journalists, will take place only with the consent of the Director of Admissions and Marketing and under appropriate supervision. When images are taken for publication by third parties, children will only be named if there is a particular reason to do so (for example if they have won a prize) and home addresses will not be given out. The information will also be checked to ensure that the child's School residence cannot be identified.

3.3. If there is any doubt about these matters, the person wishing to take the image must obtain the written consent of the child's parent(s) or, where the child is of sufficient maturity and understanding, the written consent of the child (see 6.3) and of the Designated Safeguarding Lead.

### Promotional Material

3.4. Images of students may be taken by staff and used by the School in accordance with normal custom and practice. Such custom and practice will include images of School life and associated activities. It has also been custom and practice for international schools to use images of their students for social media posts, marketing purposes, such as in prospectuses, promotional videos, internal displays, the website and occasionally through other printed and electronic materials. All families joining the School sign the School's Terms and Conditions of Enrolment to give permission for this, noting any family may remove permission by contacting the Marketing Team at any time.

- 3.5. The list of families who have refused permission for their child to appear in images used by the School is managed by the School's Marketing team. It is available to all staff through the School's shared drive (RST-Whole School Documents/Marketing/Student List- Images not to be used)
- 3.6. If a staff member would like to use an image of any student outside of normal teaching and learning usage, the list noted in 3.2.2 should be checked and if in any doubt permission should be sought from the student's family.

#### Taking of Images by Parents & Friends

- 3.7. Parents and friends often wish to take images of their children at School plays and concerts or sporting activities. Courtesy and good manners require that the following rules are respected:
  - Visitors must use their cameras with consideration and confine their photography to the relevant event;
  - If visitors ask whether they can take photographs, they should be reminded that whilst it is permissible under the Personal Data Protection Act (2019) to take photographs for personal use, publication of such images (including on personal social networking sites even where access to the image may be limited) may be unlawful;
  - Where a play or concert or other event is subject to copyright and performing rights restrictions, visitors will not be permitted to take images, photographs, or video film.

#### Seeking Consent

- 3.8. The School seeks consent for normal School use of images during the admissions process as all parents and guardians sign to accept the School's Terms and Conditions of enrolment.
- 3.9. Although further consent of parent(s) or students is not always a legal requirement, the School will seek express prior consent from students, or parents if the student is not of sufficient maturity and understanding (see 3.4.3):
  - or public use of portrait style images of individual students;
  - for use of students' images by or with commercial sponsors;
  - where a student wishes to use images of other students as part of GCSE or A-level coursework;
  - where the School might receive a payment or other tangible benefit for allowing the
  - use of a photograph, for example, providing a photograph to the media where the student has subsequently become a celebrity.
- 3.10. Where consent is required as above the School will obtain such consent from the student, provided that the student is of sufficient maturity and understanding to provide consent. If not, consent will be sought from at least one parent (see 3.4.4) noting that the School will always ask for a parent or guardian's consent if the student is under the age of 10.
- 3.11. To evidence consent, the staff member responsible for storing and using the image should keep a record of permissions received via a spreadsheet or other record.
- 3.12. Should a child or parent decide at any time the child is at the School that they do not wish photographs or images of them to be used in any of the School's promotional material they have the right to withdraw their consent and should advise the head/Deputy of this, who in turn will inform the marketing department to add the student to the list noted in point 3.2.2 above.

### Photographs as Part of Student Records

- 3.13. The School takes photographs of individual students at the start of their school career and at other key points as they transition through the School for use of their school record and on school identification cards. These images are subject to the Personal Data Protection Act (2019) and will therefore:
- be stored securely;
  - not be used for any other purpose without the consent of the student or his or her parent(s) (see 3.4.3);
  - not be shown, copied, or given to any unauthorised person.

### Use of Cameras, Video Cameras & Mobile Electronic Devices with Camera Facility

- 3.14. Students may only use cameras (of any sort) in lesson times with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- 3.15. Students may only take images with cameras (of any sort) with the express permission of all those appearing in the image. All students must allow staff access to images stored on mobile electronic devices and/or cameras and must delete images if requested to do so. Rights to privacy must be respected and images which could be construed as indecent are prohibited.
- 3.16. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. Appropriate action will be taken in accordance with the School's Acceptable Use policies (see 5).
- 3.17. Photographs of any member of the School community are not permitted to be displayed publicly around the school campus unless sanctioned by an appropriate member of staff for official use on notice boards or authorised brochures/posters, and only with the consent of the individual(s) in the image.

### Child Protection

- 3.18. When publishing images of children in School documents or on the website, care will be taken to minimise the risk of such images being modified to create inappropriate or indecent images. The Designated Safeguarding Lead can give specific advice as requested.
- 3.19. Staff will be mindful of child protection issues and will raise concerns with the Designated Safeguarding Lead if they become aware of anyone:
- taking an unusually large number of images;
  - taking images in inappropriate settings such as cloakrooms, toilets or changing areas;
  - taking images of children who are apparently unaware that they are being photographed or filmed.
  - contravening the guidance in this policy or other Rugby School Thailand policies in any way.

### Taking of Images of Students by Staff

- 3.20. Staff should use School devices where possible. However, the use of personal devices, such as phones or cameras, is permitted under guidance from the Head of School or for marketing purposes.
- 3.21. Images taken on personal devices that need to be stored for future use should be uploaded to the RST Images Repository Google Shared Drive as soon as is practicable.



- 3.22. All images taken on personal devices must be removed from the member of staff's personal device and personal cloud accounts/drives by the end of the School day. If for any reason this is not possible, the Designated Safeguarding Lead must be informed.
- 3.23. If you wish any images to be shown on any social media sites, please refer to Section 4.
- 3.24. The Designated Safeguarding Lead must be consulted if there is any doubt about taking or keeping images of children. The Designated Safeguarding Lead's decision on these matters will be final.

#### Recording Images of Students & Staff

- 3.25. Rugby School Thailand takes CCTV footage in various parts of the campus as part of the security measures used to protect our School community. These videos are stored on the server and are automatically deleted within 30 days after they were recorded. There is a facility to export footage. This is permissible for the purposes of safeguarding providing the use complies with the Section 3, CCTV policies, and the terms below.
- 3.26. Staff may volunteer to have a camera in their classroom/office. The Senior Leadership Team and the Designated Safeguarding Lead will have access to the recorded material, without needing permission from anyone else to ensure compliance with this policy and with other School policies. The Senior Leadership Team and Designated Safeguarding Lead will not access the recorded material for any other purposes other than if concerns arise..
- 3.27. The footage captured by the CCTV system is exported through the School's Safety Officer and certain IT team members only.
- 3.28. Footage of students obtained through CCTV capture will not be used for publicity or marketing purposes.
- 3.29. No content should be shared with any party outside the School without written consent from the Senior Leadership Team.
- 3.30. No footage should be exported and stored on media which is not approved or owned by the School.
- 3.31. For classrooms fitted with CCTV cameras, teachers must ensure all students in the class are aware of the camera and that it is always on. Staff should make it clear that the technology is a tool to assist in safeguarding. Students may not reasonably withhold their permission to be recorded.
- 3.32. Each classroom with lesson capture technology installed will have a sign on the wall explaining that the camera is in operation.
- 3.33. Footage will not be shared with parents or students. Any incidents that require playback of the footage as an aid shall be reported to one of the Senior Leadership Team or the Designated Safeguarding Lead, and shall be provided directly to the School's Safety Officer for any further investigations.

## 4. SOCIAL MEDIA

### Understanding Social Media

- 4.1. Social media provides platforms which enable users to interact, create and exchange information online (including those running on mobile devices). Examples include, but are not limited to, sites such as Facebook, Twitter, Instagram, YouTube and TikTok, as well as online discussion forums.
- 4.2. To capture the benefits offered by social media, Rugby School Thailand will explore and implement social media use for marketing, and educational purposes.
- 4.3. All members of staff should bear in mind that information they share through social networking applications, even if they are in private spaces, are still subject to compliance with relevant legislation.
- 4.4. All members of staff must also operate in line with the school's Equalities, Child Protection and Safeguarding, Section 3 and 5.

### Guidance on Use of Social Media

- 4.5. When using social media in a personal capacity:
  - you should make it clear that you are speaking in your personal capacity and not as our representative, communicate in a way consistent with that, and if you choose to include contact information this should be your personal, not work contact details; and
  - if you do elect to disclose your connection to us, then you must clearly and expressly state that your views do not represent those of the School.
- 4.6. *Permanent Form:* It is always useful to bear in mind when posting any Social Media content or comment that they may be permanently and publicly available and that you may not be able later to delete or remove them. You should ensure that your communications are consistent with the image that you would like to present publicly including to us and any future employers, colleagues, friends, business contacts and the world at large.
- 4.7. *Personal Liability:* Remember that you are personally responsible and may be legally liable for what you communicate on social media. Public statements of this type can create legal issues in a number of different ways including being defamatory, breach of confidentiality, infringement of intellectual property or amounting to unlawful harassment.
- 4.8. *Misunderstandings:* Before posting comments, think about whether, even if innocently meant, they could be misconstrued in a way that creates legal problems or reputational damage for us or you. Steer away from commenting on sensitive topics relating to us or your employment. Such comments might damage our reputation even if you make clear that the views you express are personal.
- 4.9. *Privacy and Confidentiality:* All of us have information that we prefer to keep private. Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission or in breach of this policy.
- 4.10. *Respecting Intellectual Property:* If you post or reference material that is protected by intellectual property rights, you should satisfy yourself that you have taken steps to avoid legal liability such as appropriately referencing sources and ensuring that citations are accurate. If

you are an Authorised Business User and have questions about whether a particular post or upload to our Social Media accounts or profiles might violate anyone's copyright or trademark, then you should check with the IT Director in advance.

- 4.11. Except for approved communication sites or applications (for example e-mail or instant messaging), the use of social media networking should be limited during the School's operational hours as directed within this policy and by the Head of School or the Principal.
- 4.12. There are many legitimate uses of social media within the curriculum and to support student learning. For example, courses may require the use of online blogs for assessment.
- 4.13. However, when using social media, the boundaries between professional and personal can become blurred and items can be capable of more than one interpretation but once published the damage may not be recoverable.
- 4.14. Heads of School and Heads of Department are responsible for either directly supplying or designating a member of their team to supply relevant encompassing and concise Social Media content to Marketing for use on all channels, including Social Media and The Rugby Post.
- 4.15. Content supplied by departments will be checked to ensure it follows school brand guidelines and is consistent with the quality of output from the official channels before being shared.
- 4.16. Under no circumstances should any staff member:
  - Take images of students on any personally-owned device without first reading the Section 3) or without seeking direct approval from the Head of School.
  - Create or manage independent social media accounts relating to the School.
  - Supply images direct to parents or students without consent from the Head of School Department Director.
  - Communicate with parents or children via social media channels.
  - Include the full name of children alongside images or display the individual child(ren)s name(s) unless deemed necessary, for example a post about the head boy/girl. If a name is included it should be first name only, unless written consent has been given by the parents for a specific circumstance.
  - Engage in posts or activities which are detrimental to maintaining effective working relationships within the school.
  - Bring the reputation of the School into disrepute.
  - Engage in activities which compromise, or might be seen to compromise, the professional standards of teaching or support staff.
  - Suggest their personal content represents the views of Rugby School Thailand.
- 4.17. Any staff members using School social media channels must:
  - Always maintain proper professional channels and boundaries with students, parents, and carers for all School-related issues; even when students, parents or carers initiate electronic interaction. (as per Staff Code of Conduct).
  - Be particularly aware of the guidelines when staff have external friendships with parents/carers. An individual is under a duty not to:
    - Disclose confidential information without express authority, especially about students, parents or carers, staff, voluntary or other workers at the school, nor breach their right to privacy.

- Share information with students or parents/carers in any environment that they would not willingly and appropriately share in a School or School-related setting or in the community.
- Post comments which incite others to make discriminatory or other professionally unacceptable comments.
- Post School logos or similar images that may lead readers of posts etc. to believe the individual is speaking on behalf of the School.
- Before posting items or communicating in social media, individuals should consider seriously whether the item is appropriate for the public domain. If there is some doubt, then it should not be posted; you may not be able to control who sees the information and how they interpret it.
- Take care that interaction on social media does not damage working relationships between members of staff, students at the School, their families, and other stakeholders and/or working partners of the School.
- Maintain professional standards by communicating with students & parents/carers electronically at appropriate times of the day and through established approved platforms.
- Not exchange private texts, phone numbers, personal email addresses or photos of a personal nature with students, parents, or carers.
- Decline student-initiated 'friend' requests and not issue 'friend' requests to students. Nor communicate with students on any social network site or similar website or forum.
- Staff should not accept any current student of any age as a friend, follower, subscriber or similar on any personal social media account until 1st September following that child leaving the School, providing the alumni is aged eighteen or above.
- Maintain a formal, courteous, and professional tone in all communications to ensure that professional boundaries are maintained.

#### Prohibited Use of Social Media

4.18. Your communications through social media, like all other modes of communication, must not breach the School's disciplinary or workplace rules or any other policy and procedure and must not cause us to be in breach of obligations we owe to others or breach any laws. For example, you must not use social media in any way that:

- breaches obligations of confidentiality which you owe to us or to any third party or which causes us to breach duties of confidence which we owe to any third party.
- breaches the rights of any other Staff member or third party to privacy, data protection and confidentiality or which amounts to bullying or harassment;
- is offensive, insulting, discriminatory or obscene;
- poses a threat to our trade secrets, confidential information, and intellectual property;
- infringes the intellectual property rights of any other person or entity;
- defames, disparages, or causes reputational damage to us or our associated companies or to any party with whom we have a business relationship, such as suppliers or parents/guardians;
- breaches or causes us to breach any law or the rules or guidelines of any regulatory authority relevant to our School;
- breaches data protection rules;
- breaches our rules, policies, or procedures for the use of our IT Systems or other equipment or resources;
- is dishonest, improper, unethical, misleading, or deceptive (e.g., pretending to be

- someone);
  - is likely to either directly or indirectly damage your reputation or our reputation;
  - breaches any of our other policies and procedures, including communications and acceptable use of equipment policy.
  - You may not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.
- 4.19. Information relating to business contacts that you make in the course of your employment amounts to confidential information and belongs to us. As such, you are not permitted to add such information (including contact details) to your personal Social Media accounts.
- 4.20. You must not give references for any person on a social media site (including any professional networking sites) on which our identity as your employer is shown in any public or private part of the site. This applies whether the reference is positive or negative. The reason for this is that such references may otherwise be attributed to us and create legal liability both for us and for you personally as the author.

#### Safeguarding Policy Compliance

- 4.21. In accordance with the School's Safeguarding Policy, the following activities must not be undertaken:
- Bullying and harassment – such conduct against any colleagues via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the School's normal bullying and harassment and/or disciplinary policies and may be treated as a criminal offence in certain circumstances.
  - Incitement of racial or religious hatred or similar activities – these may lead to criminal investigations and penalties.
  - Posting libellous statements – an individual may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by an employee could mean the school is vicariously liable for defamatory statements if carried out in the normal course of employment, even if performed without the consent or approval of the school. Similarly, making such statements on your own initiative and not at work could mean you face legal action.
  - Grooming students or similar activities to develop an inappropriate relationship(s).
  - Bring the School's reputation into disrepute.
  - Compromising the security of the School's systems.
  - Breaching confidential information about the School or any of its students, staff, governors, volunteers, or other individuals associated with the School. Do not publish anything that might allow inferences to be drawn which could embarrass or damage a student, employee, governor, volunteer, or supplier.
  - Breaches of copyright or other similar infringements – passing on text, photos etc; may infringe the owner's copyright. Always ensure that you have the permission of the owner.
- 4.22. The School takes the matters above seriously and disciplinary action will be taken. If substantiated, the normal outcome will be dismissal. A very serious view will also be taken of any individual who ignores or wilfully or carelessly carries out actions or omits to act which results in breaches of the instructions and advice contained in this policy and the result is, for example, undermining effective working relationships, professional boundaries between individuals and student similar examples in this policy.

- 4.23. Consider actions where you are 'checking in' to the School (via Facebook), as by doing this it will auto-tag the image into the School's official page. Facebook pulls in any recently tagged images to official events created.

#### Use of Personal Devices

- 4.24. Staff are allowed to bring personal mobile devices, such as phones or cameras, to School for their own use, but will limit such use to non-contact time when students are not present.
- 4.25. Staff members' personal devices should remain out of sight during contact time with students, except for the purposes of marketing where a staff member needs access to their device to capture images.
- 4.26. Staff should use School devices where possible. However, the use of personal devices, such as phones or cameras, is permitted under guidance from the Head of School or for marketing purposes.
- 4.27. Prep students are not allowed to bring personal mobile devices, such as phones or cameras, to School for their own use, unless a written parental agreement is in place.
- 4.28. Senior students are allowed to bring personal mobile devices, such as phones, to School for their own use, but will limit such use to non-contact time, unless required by a member of staff. Where applicable, these devices are subject to acceptable use (see Section 5 below)

#### Primary & Secondary Social Media Accounts

- 4.29. In general, the Marketing Department will use individual subject departments to create a dedicated hashtag, for example, #ENGLISH\_RST, #DT\_RST #ART\_RST, which can be used on content relating to that subject shared through primary marketing channels, such as the School website, Schoolzine, Facebook and Instagram accounts.
- 4.30. Content supplied by departments for social media use through primary channels will be checked by marketing to ensure it follows school brand guidelines and is consistent with the quality of output expected from the official primary channels before being shared.
- 4.31. The use of secondary School social media accounts, such as those for departments (@DRAMA-RST or @SPORT-RST etc) is permitted with written permission from the School under guidance from the Marketing Department.
- 4.32. When setting up a secondary School social media account for a department;
- a central marketing email will be used to set up all accounts, noting the account will be owned by RST not a staff member.
  - each account must have 2 members of staff and a member of Marketing as admin members.
  - all passwords and usernames should be held by the School's Social Media Manager.
  - all names and designs should be regulated by the Marketing Department.
  - content must reflect School standards noting only relevant, positive and professionally acceptable content should be posted.
  - the staff members attached to each account are tasked with ensuring anyone posting on secondary accounts is familiar with both this section and Section 3, and that all content meets policy guidelines and school standards.
  - Staff not allowed to follow the community back, or follow any personal accounts.

- The Designated Safeguarding Lead for the School will be informed about all staff members who wish to run accounts.
- 4.33. All secondary accounts must be register by staff using this process;
- Discuss and get permission from your Head of School.
  - Contact Marketing to discuss details and get the final go-ahead.
  - Complete this [Registration Form](#).
- 4.34. No other School social media accounts connected to the School should be created or managed independently.

#### School Trips or Excursions

- 4.35. We understand parents wish to see coverage of student outings and trips. In these instances, School staff should consider using:
- 4.36. Official Secondary accounts as detailed above.
- 4.37. Where deemed appropriate by the Heads of School, offer parent groups a daily report via newsletter style, collated by a key representative on any given trip and sent directly to parents through email or another official school channel such as Schoolzine push notifications.
- 4.38. Content that can be shared with our full community through the official School social media channels by the marketing team.

#### Privacy & Security Settings

- 4.39. Privacy settings can shift and change without notice. Check the settings frequently. Ensure that privacy settings for content/photos are set appropriately and monitor who can post to your social media locations and view what you post. You should not allow students to view or post on those locations.
- 4.40. Ensure your own device is configured appropriately and be mindful of your own storage configurations. For example, understand that every photo you take may be automatically synchronised to a cloud network stored elsewhere or within multiple file locations on your device.
- 4.41. Protect yourself from identity theft by restricting the amount of personal information that you give out.
- 4.42. Be cautious about posting detailed personal information such as date of birth, place of birth and favourite sports team, which can form the basis of security questions and passwords and enable personal details to be cloned for fraudulent acts etc and grooming.

#### Monitoring

- 4.43. Information stored in our IT Systems belongs to us. You should have no expectation of privacy in any communication, document, information file, post, or conversation (“Information”) that you send or receive, access, print or store using our IT Systems. In particular, we may:
- intercept, monitor and read any Information or activities using our IT Systems, including Social Media use, to ensure compliance with our rules and for our legitimate business purposes. This may include the use of recording devices or other surveillance methods, keystroke monitoring and other technologies; and

- retain copies of Information to store copies of such data or communications after they are created and delete such copies from time to time without notice.
- 4.44. Monitoring Social Media use will be conducted in accordance with an impact assessment that we have carried out to ensure that monitoring is necessary and proportionate. Monitoring is in our legitimate interests and ensures this policy is being complied with. For the purposes of the law on data protection, the Employer is a data controller of the personal information in connection with your employment. This means that we determine the purposes for which, and the way, your personal information is processed. The person responsible for data protection compliance is our Data Protection Officer.
- 4.45. Monitoring will normally be carried out by our IT Security team.
- 4.46. Personal information obtained through monitoring may be shared internally, including with members of the HR team, your line manager, managers in the business area in which you work and IT staff, if access to the information is necessary for the performance of their roles. Information is only shared internally if we have reasonable grounds to believe that there has been a breach of this policy. We will not share information gathered from monitoring with third parties unless we have a duty to report matters to a regulatory authority or law enforcement agency. Personal information gathered through monitoring will not be transferred outside of the Kingdom of Thailand.
- 4.47. You have several rights in relation to your personal information, including the right to make a subject access request and the right to have your information rectified or erased in some circumstances. You can find out more about these rights and how to access them in our Data Protection and Data Security Policy. If you believe that we have not complied with your data protection rights, you can complain to the Personal Data Protection Committee.
- 4.48. Access to social media may be withdrawn in any case of misuse (see Section 5 below)

## 5. STUDENT ACCEPTABLE USE

- 5.1. This document sets out the conditions that govern the safety of Rugby School Thailand's parents, students, staff (users) and IT equipment, specifying the responsibilities entered into by the users. Students are required to electronically sign the student version of this at the start of each academic year, which is differentiated in language for each school.
- 5.2. Students will:
- 5.2.1. only use the account provided to them by school on school computers
  - 5.2.2. only use a device when the teacher instructs them, for educational purposes, not personal, business, illegal purposes or access games or other resources that make me take part in inappropriate activities. This includes never taking photographs of anyone unless told otherwise
  - 5.2.3. when using a school device, never send personal or spam messages, mention the school in any official communication, or communicate in any way that will upset, intimate, bully or insult any person
  - 5.2.4. ensure they do not access any website that may upset them or others such as sites that are violent, racist, pornographic or illegal and reject anything they find upsetting, never respond to it and report it to a teacher



- 5.2.5. not link themselves myself or upload any images to the Web without their teacher's permission / signed parent or carer permission
- 5.2.6. correctly cite any work they use that is not their own
- 5.2.7. not bring in portable storage, install anything on school computers or contribute to any change in security and general settings
- 5.2.8. not bring in any device of their own including smart watches without permission
- 5.2.9. understand that the School can access and monitor their activities on a School linked device at all times
- 5.2.10. make sure they take care of a school device and keep it safe by:
  - not eating or drinking near it
  - only plugging the charging cable into it
  - never applying unnecessary weight to it
  - never removing its cover
  - never leaving it behind
- 5.2.11. understand they will not be able to download onto a School device
- 5.2.12. tell their teacher should they damage a device
- 5.2.13. hand their device over for checks at anytime if asked by a teacher
- 5.2.14. make sure they charge their device ready for the start of the School day
- 5.2.15. never share their passcode or password with another student
- 5.2.16. never run with a device, and always where possible, walk with its case closed
- 5.2.17. understand there are consequences as per the policy of each School, if they break this agreement

## 6. STAFF ACCEPTABLE USE

### Access

- 6.1. The School has provided computers for use by staff as an important tool for teaching, learning and administration of the School. Use of School computers, laptops and other computing devices by members of staff is governed at all times by this policy. Please ensure you understand your responsibilities and direct any questions or concerns to the Director of IT in the first instance.
- 6.2. In addition to the IT equipment provided to aid the administration and teaching and learning, all staff are provided with:
  - A School email account.
  - Access to network printers and copiers. Usage is monitored by the School.
  - Access to the MIS as appropriate to the staff role in School.
  - Connectivity to allow personal devices access to the School's wireless network.
- 6.3. Dependent on the role of staff within the School, laptops or other computing devices may be provided where appropriate. When requested by the IT department, School-owned devices should be returned to School within 48 hours of any request.

### Computer Security & Data Protection

- 6.4. All staff are provided with a personal account for accessing the computer system with a unique username and password. This account will be tailored to the level of access required and as such staff must not disclose this password to anyone.
- 6.5. Students should not be given individual use of a staff account under any circumstances.

- 6.6. When leaving a computer unattended, staff must ensure the computer is locked or the individual has logged off to prevent anyone using the account in question.
- 6.7. Staff must not store any sensitive or personal information about staff or students on any portable system unless that storage system is encrypted with an encryption software and approved for such use by the School.
- 6.8. Staff must not display sensitive or personal information on a public display or projected image. This includes student data in the MIS system.
- 6.9. Staff must make regular backups of data kept on any storage system (physical or cloud based). The departmental files and folders stored on the School shared folders will be automatically backed up and administered by the IT department.
- 6.10. When publishing or transmitting non-sensitive material outside of School, staff must take steps to protect the identity of pupils, especially when parents have requested this.
- 6.11. School-related sensitive and confidential material should only be printed to printers located in School and staff offices or the staff room.

#### Use of Staff Owned Equipment

- 6.12. If staff keep files on a personal storage device (such as a USB memory stick), all other computers that connect to this storage device should have an up-to-date anti-virus system running to prevent the proliferation of harmful software on the school computer system.
- 6.13. Personal equipment is not insured by the School. Staff should ensure any personal device has adequate insurance cover arranged to cover against loss, damage or theft.
- 6.14. It is expected that all personal devices of the staff members are running on genuine software with the appropriate licences applied. The school is not responsible in providing any form of software licensing and assurance for any privately-owned computing devices.
- 6.15. Staff members are given access to the School network with their personal computing devices.
- 6.16. The network is shared between the School stakeholders, and all staff members are expected to utilise the School network in a professional and ethical manner.

#### Conduct

- 6.17. Staff must at all times conduct computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered inappropriate are the following:
  - Using, transmitting or seeking inappropriate, abusive or offensive materials.
  - Making or inciting comments of a prejudicial or defamatory nature.
  - Installing illegal or unauthorised software onto school-owned devices.
- 6.18. Staff must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- 6.19. Staff must not intentionally damage, disable or otherwise harm the operation of computers.
- 6.20. Efforts must be taken to not intentionally waste resources. Examples of resource wastage include:

- Excessive downloading of material from the Internet.
  - Excessive storage of unnecessary files on the network storage areas.
  - Use of the smaller printers to produce bulk class sets of materials, instead of using the bulk printing photocopiers.
  - Leaving the desktop computer and Interactive LED boards on after teaching periods.
  - Excessive usage of the school-owned printers in printing personal materials.
- 6.21. The computer rooms are a whole School resource but are also the IT department teaching rooms. Please ensure all computer rooms are left in a satisfactory manner.
- 6.22. When arranging use of computer facilities for pupils, staff must ensure supervision is available. Supervising staff are responsible for ensuring that the Section 5.1 for students is enforced.
- 6.23. Staff should take care if eating or drinking around computer equipment.
- 6.24. Any damage incited by negligence on the IT equipment either assigned or borrowed to you will be investigated and the cost of repair/ replacement incurred will be your responsibilities.
- 6.25. Further, you must not:
- Delete, destroy, or attempt to modify our computer systems or any information contained on them except in line with this policy or instructions given to you by the IT Director;
  - Use our computer systems to conduct any personal business gains such as cryptocurrency mining etc.
- 6.26. You should also note that the following activities are criminal offences:
- Unauthorised access to computer materials (hacking); and
  - Unauthorised modification of computer materials.

### E-Safety

- 6.27. With the advancement in technology over the last few years, it is clear that E-Safety is an important message pupils and staff should be aware of. Rugby School Thailand is committed to providing a safe learning environment for our students and as such all staff must:
- Be aware of e-safety issues affecting students and staff through information shared by the safety leads.
  - Regularly remind pupils of key e-safety messages such as never giving out personal details online. Staff will be vigilant when asking students to search for information or images.
  - Report accidental access to inappropriate material to their line manager and any issues of child protection following the correct procedures.

### Use of E-Mail

- 6.28. The School recognises the value and importance of email as a system of directed communication and as such all staff are provided with an email address for communication both internally and with other email users outside the School.
- 6.29. Email has the same permanence and legal status as written hardcopy documents and may be subject to disclosure obligations in exactly the same way. Staff must be cautious when sending both internal and external email and the professional standards that apply to internal memos and external letters must be observed for email.
- 6.30. Staff should contact relevant line managers before contacting parents and always CC the

relevant senior teachers/ leaders as appropriate.

- 6.31. Staff should check emails periodically during the course of the School day. This should however not make assumptions that all staff will always be in a position to do this.
- 6.32. Before sending an email, consider if a different form of communication would be equally or more effective.
- 6.33. Never send an email as an angry or upset response – take time to assess the situation and talk to someone if needed for guidance or support.
- 6.34. Avoid blanket emails to all staff. If the intended audience is difficult to isolate, make this known as a sub-heading, eg, “All teachers of year 3” or alternatively make effective use of the group contacts already in place in the email system.
- 6.35. Use a clear, subject title which can be tracked.
- 6.36. Remember, emails can sometimes be misinterpreted by the receiver. Avoid emotive language and ambiguity.
- 6.37. All School email sent should have a signature containing staff name, job title and the name of the School as per the instructions sent from the Marketing department [here](#).
- 6.38. It is worth remembering that email is not a secure method of communication and can be easily copied, forwarded and archived. Unless explicitly told to do so, staff must not send, transmit or otherwise distribute proprietary information, copyrighted material or other confidential information belonging to the School.

#### Use of Video Conferencing

- 6.39. Staff will not conduct 1:1 video calls with students unless in special circumstances where the call must be recorded.
- 6.40. Any person within range of the camera’s feed must wear suitable clothing at all times.
- 6.41. Computers should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- 6.42. A live class should be recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed.
- 6.43. Language must be professional and appropriate from any person in range of the participating device’s microphones
- 6.44. The School should risk assess the use of live learning using webcams
- 6.45. Data Controllers need to reassure themselves that any teaching / learning software and / or platforms are suitable and raise no privacy issues; or use cases against the providers terms and conditions (EG: no business use of consumer products)

## Privacy

- 6.46. Use of the School computer systems, including your internet use and communications sent to you or received by you, by phone, email (including associated files or attachments), fax or any other means, will be subjected to monitoring for a number of relevant business reasons, including but not limited to:
- ensuring compliance with the terms of this policy;
  - training and monitoring standards of service;
  - ensuring compliance with regulatory practices or procedures imposed or recommended by any regulatory body relevant to our business;
  - ascertaining whether internal or external communications are relevant to our business;
  - preventing, investigating, or detecting unauthorised use of our IT systems or criminal activities
  - maintaining the effective operation of our resources - in particular, all emails received by the Employer are automatically scanned for viruses;
  - establishing the existence of facts.
- 6.47. Where it becomes apparent in the course of monitoring emails or other communications that a particular message is obviously private, we will take reasonable steps to respect your privacy in respect of that message. However, it may not be possible to determine whether that communication is personal or business-related until it is already open and read. You should therefore not have any expectation of privacy as to your use of our Resources, including communications sent to you or received by you, by phone, email (including associated files or attachments), fax or any other. If you wish to maintain the privacy of your communications, you should not use the school computer system for personal use.
- 6.48. You should avoid storing sensitive personal information on the School computer system that is unrelated to School activities.
- 6.49. Use of the School computer system indicates your consent to the above-described monitoring taking place.
- 6.50. Certain authorised employees involved in administering our resources may necessarily have access to the contents of email messages in the course of their duties. Any knowledge thus obtained should not be communicated to others, unless necessary for legitimate business reasons.
- 6.51. We may also take any action in administering email or other communications that is reasonably necessary to preserve the integrity or functionality of our resources including as part of a firewall or spam or virus protection arrangements. This could include the deletion or non-transmission of any emails or communications (including any personal communications).
- 6.52. You should note that the CCTV system monitors 24 hours a day and this data is recorded. Further details on CCTV usage and recording can be sought in our CCTV Policy.

## Confidentiality & Copyright

- 6.53. Respect the work and ownership rights of people outside the School as well as other staff or students.
- 6.54. Staff are responsible for complying with copyright law and licences that may apply to software, files, graphics, documents, music, messages and other material that is used, downloaded or copied. Even if materials on the School computer system or the Internet are not marked with

the copyright symbol ©, staff should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

- 6.55. Staff must consult a member of the IT support staff before placing any order of computer hardware, software, and online subscriptions; or obtaining and using any software believed to be free. This is to check that the intended use by the School is permitted under copyright law.

### Reporting Problems with the Computer System

- 6.56. It is the responsibility of the IT Support personnel to ensure that the School computer system is working optimally at all times and that any faults are rectified as soon as possible.
- 6.57. Staff should report any problems that need attention to a member of the IT support staff as soon as is feasible through the online Help Desk system. Problems that seriously hinder an individual's job or teaching and require immediate attention should be reported in person.
- 6.58. If staff suspect their computer has been affected by a virus or other malware, they must report this to a member of IT support staff immediately.

## 7. ONLINE SAFETY

- 7.1. Online safety resources can be accessed at any time by the community via the school's wellbeing website: [RST Wellbeing](#). These resources are kept up-to-date via the Director of Digital Learning via research and input from, but not limited to: FOBISIA, ISTEAC, ACAMIS, AppsEvents, NOS, and DiGii Social.
- 7.2. Support organisations are available as listed under "Additional advice and support" in [KCSIE 2022](#) (pages 155 - 157)

## 8. BREACHES OF POLICY

- 8.1. We must all contribute to protecting the business reputation of the School. If you see content on social media that is defamatory, false or disparages or reflects poorly on our organisation or our stakeholders, you should contact the IT Director. In the event the breach of this policy causes any loss or damage to us, or we become aware of any breach under this policy falling under the provisions of material breach in your employment agreement, in addition to our right to terminate your employment, we reserve the right to take any other legal actions and pursue any other legal rights available to us.
- 8.2. All members of staff have a duty to ensure this acceptable use is followed.
- 8.3. Staff must immediately inform a member of the IT department staff, or a member of SLT, of abuse of any part of the computer system. Specifically, staff should report:
  - Any websites accessible from within School that are unsuitable for staff or student's consumption
  - Any inappropriate content suspected to be stored on the computer system. This may be contained in email, document, pictures etc.
  - Any breaches, or attempted breaches, of computer security.
  - Any instance of bullying or harassment suffered by staff, another member of staff, or a pupil via the School computer system.

- 8.4. Staff who breach this policy:
- will be required to disclose relevant passwords and log-in information and to otherwise cooperate with our investigation;
  - may be required to remove the offending internet postings, comments, or information; and
  - may be subject to disciplinary action up to and including dismissal.

## 9. APPENDICES

9.1. The following policies are currently defined as requiring separate review processes and are consequently appended to the Digital Awareness Policy as opposed to being integrated. This is subject to review and amendment from the upcoming Digital Wellbeing Team; a subset of the EdTech Team as per Phase 1 of the Digital Learning Strategic Plan.

- [CCTV Policy](#)
- [Data Breach Policy](#)
- [Data Protection Policy](#)
- [Information Protection & Handling Policy](#)
- [Privacy Policy](#)
- [Data Retention Policy](#)
- [Data Classification Policy](#)



RUGBY SCHOOL  
THAILAND

