SOCIAL MEDIA POLICY

Statement of policy and purpose of Policy

1. Thai-Chinese International School (TCIS) (the "**Employer**") recognizes that social interaction on the internet is an important and integral part of life and, if used correctly, can offer valuable business opportunities. However, inappropriate use of social media can be a serious drain on productivity and can also pose significant business risks.
2. It is our policy that staff may make limited use of social media during their hours of work, as set out in this policy. In addition, the use by staff members of social media at any time, and whether or not using our equipment, must comply with the rules set out in this policy if it may affect our business in any way.
3. The purpose of this policy is to ensure that all staff understand:
   a. the extent to which personal use of social media is permitted during hours of work;
   b. the limitations on their use of social media, whether used during or outside hours of work; and
   c. the types of use of social media that could expose them and us to legal liability.
4. This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

Who and what does this policy apply to?

5. This policy and the rules contained it in apply to:

a. all our staff, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants, and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (the "**Staff**");

b. use by Staff of websites specifically aimed at social interaction such as Facebook, LinkedIn, Wikipedia, and Twitter as well as blogging, participation in wikis and the use of interactive features or the ability to post or publish comments or information (including video, audio, photographs and text) with other people on other websites (**social media**);

c. use of social media for business and/or personal purposes, whether or not during working hours and irrespective of whether our equipment or resources are used.

6. This policy should be read in conjunction with our Data Protection and Data Security Policy. Other policies that should be read in conjunction with this policy include:

   a. Communications and acceptable use of equipment policy.

Who is responsible for this policy?

7. The IT Director has general responsibility for the oversight and updating of this policy. All Staff have personal responsibility to ensure compliance with this policy. Managers have special responsibility for leading by example, ensuring that members of Staff are familiar with this policy and for monitoring and enforcing compliance.

Business and personal use of social media

8. All media enquiries (including requests for comments for publication on social media) should be directed to the Head of Marketing If you are contacted by a media representative or asked for comment for publication about us or otherwise in connection with your employment, you should not respond unless you have been given written approval by the IT Director.

9. Only Staff specifically authorized by the IT Director (**Authorized Business User**) may use social media on our behalf as an organization or otherwise or post comments on any of our Social Media accounts or profiles. If you are authorized to do this, then we may require you to undergo training before undertaking such activities and you will be required to comply with additional guidance and instructions concerning these communications.

10. We allow Staff to make occasional personal use of social media while at work and using our IT or communications resources and equipment (**IT Systems**), so long as all use complies with this policy and does not interfere with the proper performance of work duties.

Guidance on use of social media

11. **Personal capacity:** Unless you are an Authorized Business User, when using social media:

a. 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

b. 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 Employer.

12. **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.

13. **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 for being defamatory, breach of confidentiality, infringement of intellectual property or amounting to unlawful harassment.

14. **Taking care to avoid 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.

15. **Respecting 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.

16. **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 Authorized 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 IT Director in advance.

Prohibited uses of social media.

17. Your communications through social media, like all other modes of communication, must not breach our 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 beach any laws. For example, you must not use social media in any way that:

a. 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.

b. breaches the rights of any other Staff member or third party to privacy, data protection and confidentiality or which amounts to bullying or harassment;

c. is offensive, insulting, discriminatory or obscene;

d. poses a threat to our trade secrets, confidential information, and intellectual property;

e. infringes the intellectual property rights of any other person or entity;

f. 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 customers;

g. breaches or causes us to breach any law or the rules or guidelines of any regulatory authority relevant to our business;

h. breaches data protection rules;

i. breaches our rules, policies, or procedures for the use of our IT Systems or other equipment or resources;

j. is dishonest, improper, unethical, misleading, or deceptive (e.g., pretending to be someone);

k. is likely to either directly or indirectly damage your reputation or our reputation;

l. breaches any of our other policies and procedures, including communications and acceptable use of equipment policy.

18. 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.

19. Information relating to business contacts that you make in the course of your employment amounts to confidential information and belong to us. As such, you are not permitted to add such information (including contact details) to your personal Social Media accounts.

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.

Monitoring

21. 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**") which you send or receive, access, print or store using our IT Systems. In particular, we may:

a. 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 use of recording devices or other surveillance methods, keystroke monitoring and other technologies; and

b. 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.

22. 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 manner in which, your personal information is processed. The person responsible for data protection compliance is our Data Protection Officer.

23. Monitoring will normally be carried out by our IT Security team.

24. 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 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.

25. You have a number of 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, which you can find here: www.tcis.ac.th/privacy . If you believe that we have not complied with your data protection rights, you can complain to the Personal Data Protection Committee.

26. Access to social media may be withdrawn in any case of misuse.

27. Please refer to our Communications and acceptable use of equipment policy for more information.

Breaches of this policy

28. We must all contribute to protecting the business reputation of the Employer. If you see content in social media that is defamatory, false or disparages or reflects poorly on our organization 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 fall 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.

29. Staff who breach this policy:

    a. will be required to disclose relevant passwords and log in information and to otherwise co-operate with our investigation;

    b. may be required to remove the offending internet postings, comment, or information; and

    c. may be subject to disciplinary action up to and including dismissal.

Other relevant policies

30. Staff are referred to the Staff Handbook for other policies and procedures which may be relevant to the issues covered in this policy.