SHREWSBURY INTERNATIONAL SCHOOL
HONG KONG

Policy Title:	Digital Citizenship
Policy Section:	Section C: Curriculum
Publish to:	Policy Compendium Parent Portal Staff Portal Website

Introduction

Shrewsbury International School Hong Kong highlights Care and Compassion as a core value within Guiding Statements that also describe a 'student centred' and 'holistic' approach, 'inspired by the very best of British education'. An unwavering commitment to the wellbeing of every child in our care is also embedded deep within a Motto that connects all Shrewsbury schools: intus si recte ne labora - if the heart is right, all will be well.

Through the widespread implementation of digital networks, the world is growing ever-more interconnected. As such, it is critical that young people learn to navigate the digital world effectively, efficiently and safely. We understand the pressures that young people face in the modern world and embrace our responsibility for ensuring that they learn to navigate the challenges they are likely to face.

This policy is designed to encourage the safe and responsible use of technology and safeguard digital engagements facilitated by the internet.

Shrewsbury International School Hong Kong is fully committed to keeping every child safe - everywhere.

17th February 2025

Key Terms

'Digital Citizenship' is a recognition of the interconnection we share with others through technological means.

'Social Media' is a broad term for the group of online platforms that enable users to interact with one another.

Approach

Shrewsbury International School Hong Kong is committed to providing students and parents with the knowledge, skills and opportunities required to become outstanding Digital Citizens. It provides a wide range of infrastructural support to minimise risk and safeguard students. Through the delivery of a broad and progressive programme of study, we support students to engage with technology responsibly, to learn, create and connect.

Our Digital Citizenship programme is guided by the UK Council for Internet Safety and their Education for a Connected World framework. Alignment encourages us to focus upon eight different aspects of online engagement:

1. Self-image and Identity:
   Students explore the differences between online and offline behaviour and consider the impact of online technologies on self-image and identity.

2. Online relationships:
   Students identify strategies for developing positive relationships online and explore how technology influences the way in which we communicate.

3. Online reputation:
   Students learn how to manage their personal profile online and share content safely.

4. Online bullying:
   Students consider the impact of negative behaviour online and learn how to report and intervene effectively.

5. Managing online information:
   Students learn how to find, identify and interpret information online and consider how to evaluate information critically.

6. Health, wellbeing and lifestyle:
   Students explore the broader impact of technology and explore strategies which promote productive and positive use of technology.

7. Privacy and security:
   Students consider how personal online information can be used, stored, processed and shared.

8. Copyright and ownership:
   Students learn about the concept of ownership of online content and consider how they might best protect personal information.

In order to best equip students, the School provides a broad and progressive Digital Citizenship education programme that is fully embedded within our Computing Curriculum. Lessons encourage students to:

- Engage safely and demonstrate good judgement;
- Validate the accuracy of information available online;
- Be critically aware of any materials and content they may gain access to;
- Develop an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

To best facilitate their journey, members of staff engage positively and productively with technology in order to ensure that good Digital Citizenship is routinely modelled. The School manages a filtered internet service for all devices logged into the main school network.

Social Media

The influence of social media has grown increasingly pervasive. While keen to acknowledge the many benefits associated with wider access and improved connectivity, we remain alert to the many and varied risks associated with premature access to social media and advise strongly against it. Information shared on social media platforms is often easy to manipulate and difficult to retract.

Members of staff are reminded that they are both responsible and liable for their behaviour online and through social media. They are asked to take particular care when engaging on behalf of or in association with the School, in recognition that the same laws, professional

expectations and guidelines for interacting with students, parents, alumni, media and other stakeholders apply online as elsewhere. Their use of social media must not compromise the responsibilities they hold towards the safety and wellbeing of students.

Official School Accounts

Official school accounts can be identified through direct association with Shrewsbury International School Hong Kong. Managed by the Marketing Team, access is authorised as appropriate on a case-by-case basis. Use of the school logo, name and brand are bound by a unique agreement with Shrewsbury School. An account opened on behalf of the School is understood to belong to the School and can be closed without notice at the discretion of the Senior Leadership Team.

School accounts are regularly maintained and closely monitored to ensure that content is appropriate, representative and of sufficient quality. Accounts left dormant for a period of six months will be closed by the Marketing Department.

All members of the community are encouraged to engage positively and proactively with official school accounts.

Acceptable Use Agreement

Members of the school community accessing digital equipment independently are required to agree to the terms outlined within an Acceptable Use Agreement (AUA).

Students in Key Stage 2 are introduced to their AUA (Appendix A) during the first Computing lesson of each academic year.

Parents have the opportunity to work through their AUA (Appendix B) within a workshop delivered in the first half term of each academic year - agreement is gathered through the acceptance of Terms and Conditions.

Members of staff accept responsibility for adherence to their AUA (Appendix C) through the signing of a Code of Conduct at the beginning of each school year.

Related Policies

This Policy should be read alongside:

- B2: Terms and Conditions
- E1: Child Protection and Safeguarding
- F3: Disciplinary
- F8: Data Protection
- F11: Speak Out
- F12: Code of Conduct

The successful implementation of this policy supports the wider assessment of our achievement in relation to our Guiding Statements (A1), with Acceptable User Agreement acceptance identified as a key performance indicator.

17th February 2025

Appendix A: Student Acceptable Use Agreement

In order to be a responsible Digital Citizen, I understand and agree that:

1. Technology is provided at the School to support my education;
2. We are all responsible for taking care of the hardware made available to us;
3. Websites can contain inappropriate material for someone of my age;
4. I should report anything that I find online that makes me feel uncomfortable;
5. My words and actions online can cause harm and offence;
6. Poor online behaviour will be managed in the same way as poor offline behaviour;
7. We are all responsible for the immediate reporting of poor behaviour;
8. My use of the internet is monitored whilst I am on the school campus;
9. I need to give credit to others when I use or reference their work and consider my own digital footprint.

10. Students require the explicit permission of an adult to:
    - 10.1. Use the internet;
    - 10.2. Play games online;
    - 10.3. Download multimedia files from the internet;
    - 10.4. Use or download new applications;
    - 10.5. Turn on the camera of any given device;
    - 10.6. Photograph, video or record material;
    - 10.7. Share photographs, videos or recordings captured.

I pledge to be a positive Digital Citizen and understand that this agreement is designed to keep me safe.

17th February 2025

Appendix B: Parent Acceptable Use Agreement

Through acceptance of the Terms of Conditions (B2) associated with the enrolment of their child or children at Shrewsbury International School Hong Kong, parents acknowledge that:

1. Internet access presents both risks and opportunities;
2. Premature access to social media can have severe negative consequences;
3. They are responsible for monitoring the relationship their child has with technology and any engagements they may share with others online outside of school hours;
4. They are responsible for the safe and considerate use of technology whilst on the school campus;
5. Their online behaviour and the relationship they share with technology will have a significant influence on their child.

And act to confirm that:

1. They have read and understood the Digital Citizenship (C7) policy, to include the Student Acceptable Use Agreement;
2. They will utilise the information held within the Digital Citizenship (C7) policy to support the School in ensuring that their child is an outstanding Digital Citizen.

17th February 2025

Appendix C: Staff Acceptable Use Agreement

Through acceptance of the Code of Conduct (F12), members of staff accept responsibility for adherence to the Staff Acceptable Use Agreement on the understanding that failure to do so could result in the instigation of disciplinary action.

1. Safeguarding

    1.1. Members of staff have a duty to report when there is a cause to suspect that a student is being abused or is at risk of abuse - all concerns must be reported to the Designated or Deputy Designated Safeguarding Lead immediately;

    1.2. If a member of staff is either subject to or observes abusive, harmful, illegal or inappropriate behaviour by an adult member of the school community online, they should report it immediately via the Speak Out (F11) Policy;

    1.3. Members of staff are required to promote the safe use of digital technology in accordance with the information held within the Digital Citizenship (C7) Policy.

    1.4. Members of staff accept responsibility for the provision of explicit permission when students are required to:

        1.4.1 Use the internet;
        1.4.2 Play games online;
        1.4.3 Download multimedia files from the internet;
        1.4.4 Turn on the camera of any given device;
        1.4.5 Photograph, video or record material;
        1.4.6 Share photographs, videos or recordings captured.

2. Data Protection

    2.1. Members of staff must acknowledge and accept that the personal information they have access to is protected under the Personal Data (Privacy) Ordinance of the Hong Kong Special Administrative Region;

    2.2. Members of staff are required to comply with the Data Protection (F8) policy and report potential data breaches or cyber security threats to the IT Department at the earliest possible opportunity;

2.3. Members of staff should not disclose their Username or Password to anyone else and must lock their screen or log out of a given device when unattended in order to prevent unauthorised access to school systems and data;

2.4. The sharing of sensitive data must be limited by professional necessity and undertaken with caution - members of staff should not access sensitive data, information or material in public;

2.5. Members of staff acknowledge that the information held on emails is highly vulnerable to leaked confidential information.

3. Behaviour

3.1. Members of staff are expected to follow the same behavioural standards when interacting with technology as they would in real life - they acknowledge that written messages can be easily misconstrued and must be considerately phrased;

3.2. Members of staff are advised to consider the way in which their reputation and the reputation of the School might be affected by the content they share, link to or embed;

3.3. Members of staff must protect confidential and proprietary information about Shrewsbury International School Hong Kong and its community.

4. The School Network

4.1. Members of staff are required to use the School Network primarily for reasons connected to their employment - the School monitors the use of the School Network by all members of staff both within and beyond school hours and reserves the right to share access to relevant data with external agencies in the case of a formal or legal investigation. Inappropriate use of the School Network may result in disciplinary action in accordance with the Disciplinary (F3) policy;

4.2. Members of staff are not permitted to access software that bypasses the filtering or security systems in place that act to protect The School Network;

4.3. Members of staff are required to consult the IT Department prior to the download or upload of large files which may limit use of the School Network.

5. School Owned Devices

5.1. Members of staff are responsible for the safe use and storage of School Owned Devices - they must report damage or faults observed to the IT Department at the earliest possible opportunity;

5.2. Members of staff are required to seek the support and approval of the IT Department prior to the installation of new software on School Owned Devices.

6. Social Media

6.1. Members of staff must not identify students by their full name on social media;

6.2. Members of staff should demonstrate respect, care and caution when using photographs of students for marketing purposes;

6.3. Members of staff must check digital content featuring students with the Marketing Team prior to publication.

7. Personal Use

7.1. Members of staff are permitted to use the School Network and School Owned Devices to send and receive personal messages, provided that it does not interfere with their work;

7.2. Members of staff should not open emails or attachments from unknown or untrustworthy sources - any concerns relating to the potentially malicious software must be reported to the IT Department at the earliest possible opportunity.

7.3. Social Media

7.3.1 Members of staff should not initiate or keep contact, interact, follow or engage with students through personal social media accounts - requests must not be accepted and private messages declined;

7.3.2 Members of staff should not share messages or imagery that threatens their professional reputation or the reputation of the school;

7.3.3 Members of staff are advised to be respectful, non-confrontational and supportive of the work of the School when engaging in a personal capacity through social media;

7.3.4 Members of staff are advised to limit access to personal social media accounts wherever possible.