SYDNEY JAPANESE INTERNATIONAL SCHOOL
シドニー日本人国際学校

CYBER SAFETY　POLICY

Sydney Japanese International School

Cyber Safety Policy

1. Definition

Cyber safety refers to the safe and responsible use of information and communication technologies. This includes privacy and information protection, respectful communication and knowing how to get help to deal with online issues.

Common cyber safety issues include:

- **Cyberbullying** - the ongoing abuse of power to threaten or harm another person through the use of technology (Refer to our Bullying Prevention and Intervention policy)
- **Sexting** - the sending or posting of provocative or sexual photos, messages or videos online
- **Identity theft** - the fraudulent assumption of a person's private information for their personal gain. Students are exposed to these risks as they are often unaware of the safety issues surrounding their digital footprint
- **Predatory behaviour -** where a student is targeted online by a stranger who attempts to arrange a face to face meeting, in an attempt to engage in inappropriate behaviour.

Cyber safety issues most commonly occur through a student's use of their own technology devices (e.g. smartphone, tablet, laptop, home computer).

Safe use of technology whilst at the School is managed through our Information and Communication Technology (ICT) policy.

2. Sydney Japanese International School's Policy

Sydney Japanese International School recognises its duty to students to provide a safe and positive learning environment which includes the responsible use of information and communication technologies.

It is our policy that:

- Cyber safety be managed through a 'whole-of-School community' approach involving students, staff and parents/carers
- Cyber safety and cyberbullying prevention strategies be implemented within the School on a continuous basis with a focus on teaching age

- Appropriate skills and strategies to empower staff, students and parents/carers to recognise cyber safety issues and respond appropriately
- Cyberbullying response strategies be tailored to the circumstances of each incident
- Our bullying prevention, intervention and cyber safety strategies are reviewed on an annual basis against best practice.
- Schools have the right to monitor, track and review all content sent and received on school systems.
- Non-compliance with acceptable uses of ICT will lead to disciplinary action.

3. Cyber Safety Strategies

Sydney Japanese International School recognises that the implementation of whole of School cyber safety strategies is the most effective way of minimising risks related to our students engaging in online activity.

The following initiatives form part of our overall cyber safety strategy within the School:

- A structured curriculum that provides age-appropriate information and skills relating to cyber safety (including cyberbullying) to students over the course of the academic year
- Education, training and professional development of staff in cyber safety strategies
- Regular provision of information to parents/carers to raise awareness of cyber safety as a School community issue. This will equip them to recognise signs of cyber safety risks, as well as to provide them with clear paths for raising any concerns they may have relating to cyber safety and/or cyberbullying directly with the School
- Promotion of a supportive environment that encourages the development of positive relationships and communication between staff, students and parents/carers
- Promotion of responsible bystander behaviour amongst students, staff and parents/carers (this may occur where a bystander observes inappropriate online behaviour either being perpetrated by, or targeted at, a student
- All students' logins and passwords are protected and cannot be accessed by others.
- To support schools, teachers, staff, parents and carers to help protect students, the School is supported by experts in eSafety with evidence based advice. Topics include media, misinformation, scams, parental controls, unwanted contact, cyberbullying, online gaming and advise on self-care. (https://www.esafety.gov.au/).
- Access to the school network is provided through filtered services. Designed to restrict access to inappropriate sites, spam and virus protection.

- Ensure school approval is sought when connecting personal ICT equipment to school network equipment and devices to avoid the risk of malware.
- Regular risk assessments of cyber safety within the School are ：
    - Undertaken by surveying students to identify cyber safety issues
    - Records of reported cyber safety incidents are maintained and analysed, in order to identify systemic issues and to implement targeted prevention strategies where appropriate. All reports are recorded in the Sentral.
    - Cyber safety posters are displayed strategically within the School
    - Promotion of student cyber safety awareness by participating in relevant cyber safety related events
    - Managed through a device management system called Securely Classroom during the lessons, so teachers can safeguard each student engagement on line. Securley Classroom system is used for Year 3-6 (International Division)

4. Staff Responsibilities

All staff must:

- Model appropriate online behaviour at all times
- Refer any cyber safety related issues to the Principal or Heads
- Acknowledge the right of parents/carers to speak with School authorities if they believe their child is being bullied.

5. Parents responsibilities

Parents are expected to:

- Supervise their children's use of IT devices and online content at home.
- Refrain from sharing photos, videos, or recordings of other students without permission from their parents.
- Contact the school promptly if they accidentally access inappropriate websites, notice suspicious behaviour, or observe signs of cyberbullying.

6. Signage:

- Cyber safety posters are displayed strategically around the School.

7. Data Protection and Privacy Measures

At Sydney Japanese International School, we are committed to protecting the personal data and privacy of our students, staff, and families. We recognise the importance of handling personal information responsibly and are dedicated to ensuring that data

collected and stored on school systems is secure and managed in compliance with data protection laws and best practices.

1. **Commitment to Data Privacy**
   We collect and manage personal information only as necessary for educational and administrative purposes. This information is handled in line with applicable data protection legislation, including the Privacy Act and any relevant school policies.
2. **Secure Storage and Access Control**
   Student and staff information is securely stored and managed on school-approved systems. To prevent unauthorised access, loss, or misuse, it is protected by password-secured systems and managed through secure servers and firewalls.
3. **Use of Data for Educational Purposes**
   Personal data collected by the school will only be used for legitimate educational, administrative, and support purposes. The school does not disclose personal information to external parties without consent unless required by law.
4. **Data Retention and Disposal**
   Personal data is retained only as long as necessary to fulfill its purpose or as required by law. Once data is no longer needed, it is securely disposed of to protect privacy.
5. **Regular Review of Data Protection Practices**
   Our data protection practices are reviewed regularly to ensure compliance with evolving legal standards and to enhance our data security measures as needed.

By following these principles, Sydney Japanese International School aims to maintain a safe, transparent, and trustworthy environment in compliance with Australian federal law and NSW state law, ensuring that the personal information of school stakeholders is respected and protected.

8. Implementation

This Policy is implemented through a combination of:

- Staff training
- Education of students and parents/carers and information sharing
- Effective incident reporting forms and procedures
- Effective management of incident cases relating to inappropriate ICT use and reported cyber-safety
- Regular inspection of ICT equipment and networks
- Effective observation, record keeping procedures and assessments
- Implementation of corrective actions where necessary