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

ICT POLICY

（Rules on the use of Information and Communications Technology for Staff）

ICT POLICY

Sydney Japanese International School's policy

Students have the right to learn in a safe environment, including when they have access to ICT to enhance their learning. Sydney Japanese International School is committed to the responsible and educational use of ICT and to the protection of students by providing secure access to these services as part of their learning experience.

Staff are responsible for the use of school equipment and systems and the handling of social networks and manage them carefully (cooperating with parents). Departure from compliance with this Code may only be authorised by the Principal, General Manager (GM) and Heads.

All staffs and contractors using School Systems must comply with this Code.

All staff and contractors using the school's systems must comply with this Code, which may create a hazardous situation if ICT-related school systems are used inappropriately or illegally. Any failure to comply with this Code will be subject to disciplinary offences unless authorised by the Principal or General Manager.

It is our policy that:

- the use of ICT be managed through a 'whole-of-School community' approach involving students, staff and parents/carers
- ICT education 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 ensure appropriate use in line with the relevant curriculums.
- staff establish positive role models in use of ICT
- appropriate use of ICT (both at school and at home).
- The School may conduct the surveillance for any purpose – including to determine if you or any other person has, or may have, breached their obligations to the School or should be subject to disciplinary action.
- our ICT policy is reviewed regularly against best practice.

Code of Conduct for information and communication technology

1. Introduction to this Code

1.1.Application

This Code applies to the use of all Information and Communication Technology (ICT). The school manages school telephones, any electronic device or application (including use of the local or hard drive) used to communicate, create, disseminate, store or manage information such as text, images, audio or video and the way of SNS usage.

Examples of school ICT system include:

- personal computers and laptops
- mobile devices such as mobile phones and tablets
- applications such as email and the internet
- web-based tools such as social networking sites, chat rooms, blogs,
- instant messaging systems
- imaging tools such as video, still or web cameras and related software
- audio tools such as audio recording devices, iPods, and related software
- Smartboard
- applications such as monitoring
- scanning and copying machines
- Online educational subscriptions

1.2. Consequences of breach of this Code

Use of school systems in a manner inconsistent with this Code or in any other inappropriate manner may result in the School taking whatever disciplinary action it considers appropriate. This provision must be complied with when using social media as well. Disciplinary action may include, but is not limited to, limitation or removal of access to school systems or termination of an employee's employment or contractor's engagement with the School.

2. Responsibilities of Staff

2.1. Accountability and care of equipment

You must use the School's equipment carefully, and follow all instructions about how to use it and how to take care of it.

All users are issued with a unique username and password. (The Mobile Device supplied is managed by number). You are solely accountable for all actions performed under your username and password.

The School may hold you responsible for any:

1) damage to the School's equipment caused by your use of school systems or loss of School devices provided by the School;
2) costs incurred by your access of internet sites; and/or
3) legal obligation to any person created by your use of school systems.
4) when using internet and electronic communications, you must: always identify yourself clearly and honestly;
5) not tell anyone your password except as required by the School; and
6) never access another person's email or internet account without that person's permission or the permission of the School

Staff must:

【Accountability and equipment management 】

- School systems are a business tool, and must only be used for the school's business purposes, except as otherwise set out in this Cod
- sign and submit the ICT consent form
- return all devices provided by the school you when withdraw your employment
- model appropriate behaviour at all times
- ensure all students understand they will face disciplinary action in the event they misuse ICT equipment and devices
- ensure that students who do not return their ICT Agreements do not use ICT equipment and devices
- be vigilant in monitoring students when using ICT equipment and devices
- reinforce to students the importance of privacy and safeguarding their login details, personal information and the personal information of others
- assist students if they have inadvertently accessed inappropriate material, received inappropriate messages or if they have been offended by another person's use of ICTs

- deal with all reported and observed incidents of inappropriate ICT use in accordance with this Policy
- ensure that any incident of inappropriate ICT use that they observe or is reported to them, is recorded appropriately.
- If technical problems are derived, contact the IT support team or a contracted external IT consultant.

2.2. Viruses

All external files and attachments must be virus checked using installed scanning software before they are accessed. Virus checking is done automatically through the software installed on the mail server. If you are concerned about an e-mail attachment, or believe that it has not been automatically scanned for viruses, you should contact the Office・IT support team or contracted IT consultant

You must not knowingly introduce a virus to the school systems

2.3. Personal and other uses

The School may cease to allow such other uses at any time. Excessive use of the telephone, e-mail, internet facilities or computer systems for personal reasons may result in disciplinary action, which may include, but is not limited to, limitation or removal of access to school systems or termination of an employee's employment or contractor's engagement with the School.

2.4 Monitoring

The School may conduct the surveillance for any purpose – including to determine if you or any other person has, or may have, breached their obligations to the School or should be subject to disciplinary action.

Surveillance in accordance with this policy will commence on the Surveillance Date (if you are a new employee, the commencement date of your employment; or otherwise 14 days from the commencement date of this policy).

3. ICT Misuse Prevention

The School recognises that the implementation of whole-of-School prevention strategies is the most effective way of eliminating, or at least minimising incidents of misuse of ICT within our community.

The following initiatives form part of our overall ICT strategy:

- a structured curriculum and peer group support system, that provides age-appropriate information and skills relating to ICT use to students over the course of the academic year
- education, training and professional development of staff in appropriate ICT use
- the regular provision of information to parents/carers to raise awareness of inappropriate use of ICTs as a School community issue
- the promotion of a supportive environment that encourages the development of positive relationships and communication between staff, students and parents/carers
- all student login details and passwords are to be kept confidential to prevent others accessing their accounts
- access to School networks is provided through a filtered service. The filter is designed to restrict access of inappropriate material as well as providing spam and virus protection.
- approval must be sought before connecting privately owned ICT equipment and devices to School networks to avoid the risk of malware
- prevention of inappropriate usage by students including:
    - participation in non-educational activities such as the purchase and/or sale of products or services
    - illegal activities such as threatening the safety of others or engaging in criminal activity
    - tampering with or damaging computer hardware or software
    - making, installing or downloading copies of software that is not licensed by the School

The school must:

- any inappropriate internet sites accidentally accessed, incidents where students are offended by another person's use of ICTs and suspected technical security breaches must be immediately reported for investigation and recorded in the Sentral.
- appropriate copyright clearance is sought, and the source of any information used or published is acknowledged, to avoid plagiarism
- the School reserves the right to monitor, traffic and review all content sent and received on the School systems
- breaches of acceptable usage of ICT will result in disciplinary action
- regular risk assessments of inappropriate ICT use within the School

records of reported incidents of ICT misuse are maintained and analysed in order to identify persistent offenders and to implement targeted prevention strategies. The report is recorded in the Sensus.
- posters promoting appropriate ICT use are displayed strategically within the School

4. Permitted and Prohibited Uses of School Systems

4.1. Permitted uses: Business purposes

School Systems are a business tool, and must only be used:

1) for the School's business purposes, except as otherwise set out in this Code; and
2) in a professional, appropriate and lawful manner.

4.2. Personal and other uses

The School may, as a matter of discretion, allow use of School Systems for other purposes including personal use, so long as this does not:

1) contravene other parts of this Code or the School's policies; or
2) adversely impact on the performance of work duties.

4.3. Prohibited uses

School Systems must not knowingly be used to:

1) send or receive material that is, or may be construed to be, obscene, derogatory, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive or excessively personal;
2) send or receive material which harasses or promotes hatred or discrimination based on any unlawful grounds against any person (refer to the School's Anti-Bullying Policy);
3) injure the reputation of the School or cause embarrassment to the School;
4) send or receive material relating to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity;
5) spam or mass mail or to send or receive chain mail;
6) infringe the copyright or other intellectual property rights of another person;

7) play games;

8) game, wage or bet;

9) send or receive spam or bulk or chain mail

10) infringe copyright or intellectual property rights belonging to others

11) contribute to electronic bulletin boards;

12) perform any activity using an anonymous or misleading identity;

13) engage in any other illegal or inappropriate activity;

14) provide services or produce materials for commercial gain; or

15) Access social networking sites including, but not limited to, Facebook, Twitter, MySpace and LinkedIn (but not limited to) unless you have been specifically authorised to do so by the Principal and delegates (see Section 7, Social Networking)

4.4. Downloading of software

Software (licensed, shareware, freeware, evaluation or otherwise) including system, application or data files may only be downloaded using procedures approved by the ICT consultant.

5. Logging and Monitoring

The School notifies you that it will carry out ongoing, intermittent surveillance of your use of the School Systems – including emails, internet and files (including files stored on your work computer).

The surveillance is carried out by all means available to the School which may include:

1) accessing your work computer, email account or emails, files, storage devices and communication devices;

2) accessing records of internet usage by you (including sites and pages visited, files downloaded, video and audio files accessed and data input); and

As part of its monitoring and logging of School Systems, the School may:

5.1. stop e-mails from entering or leaving its e-mail system if it believes it is appropriate to do so, e.g. if they are offensive or otherwise inappropriate, not work-related or wasteful of electronic resources (such as mass e-mailings); and/or

5.2. block your access to particular internet websites.

6. Dealing with E-mails

6.1. School Property

The School is the owner of copyright over all e-mail messages created by its employees as part of their employment.

6.2. Inappropriate e-mails

You and/or the School may be liable for what you say in an e-mail message.

An e-mail that may seem harmless to you may be highly offensive to someone else. The audience of an inappropriate comment in an e-mail or blog may be unexpected and extremely widespread; e-mail is neither private nor secret. It may easily be copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation.

If you receive an e-mail which you think may be inappropriate, delete it immediately and do not forward it to anyone else.

6.3. Confidentiality and security

When an e-mail or Blog is sent from the School to the network server and then on to the internet, the e-mail message may become public information. You should encrypt e-mail messages /protect which contain sensitive information before sending. If you need more information about encrypting messages, you should contact the management.

Items of a highly confidential or sensitive nature should not be sent via e-mail, even with encryption.

E-mail may be truncated, scrambled, delayed, sent to the wrong address or not arrive at all. If outgoing e-mail is important or urgent, you should verify that the recipient has received the e-mail in its entirety.

When your computer is not in use it is your responsibility to ensure no information is left on your screen for others to read or take note of.

6.4. Representing the School

When sending e-mail messages for the School's business purposes, you must ensure that:

1) any representations made are those of the School; and

2) the manner of expression used is consistent with the relevant business purpose.
3) the image used is not deviated from personal privacy (especially for students' photos/video) and obtained the permission to use

Comments that are not appropriate in the workplace will also be inappropriate when sent by e-mail or posted in the blog. As noted above, any messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner. Highly recommended to be supervised the content by management before sending or posting if you have concerns.

6.5. Disclaimer

In light of these issues, you must ensure that all e-mails that are sent from your e-mail address contain the School's standard disclaimer message, which reads as follows:

Disclaimer:
This message contains privileged and confidential information intended only for the use of the addressee named above. All communications and personal information provided, are subject to the SJIS privacy policy. If you have received this message in error, please notify Sydney Japanese International School. Any views expressed in this message are those of the individual sender and do not necessarily represent the opinion of the Sydney Japanese International School. The sender cannot guarantee that this email or any attachments to it is free of computer viruses or other conditions.

6.6. Absences

If you are likely to be absent from work for any lengthy period of time, you should make arrangements for your e-mails to be accessible by the School or ensure that an 'out of office reply' is automatically set.

7. Social networking

Accessing social network sites on School Systems

As outlined in the ICT Code of Use, you are not permitted to use social networking sites on School Systems unless you have been specifically authorised to do so by the Principal, GM or Heads.

If you have been authorised to access Social Media using School Systems the Code will apply to any such access. In particular any use of Social Media on School Systems will be subject to the logging and monitoring referred to in

section 5 of the Code. You should not have any expectations of privacy for any actions performed on Social Media sites using School Systems.

7.1 Application

This Policy applies to employees and contractors when they participate in social networking sites whether during work hours or outside of work hours on their own computers or other electronic communication technologies or on School Systems if they have been authorised to do so.

This Policy covers all current and future social media platforms. These platforms currently include, but are not limited to:

a) **Social networking sites**: Facebook, X, YouTube, Instagram, LinkedIn, Tik Tok, What's up;

b) **Video and photo sharing websites**: Flickr, Instagram, PhotoBlog and YouTube;

c) **Micro-blogging sites**: X, Pinterest, LinkedIn;

d) **Blogs**: including corporate blogs and personal blogs or blogs hosted by traditional media publications;

e) **Forums and discussion boards**: e.g. local discussion boards, Whirlpool, Yahoo! Groups or Google Groups, Quora;

f) **Online encyclopaedias**: e.g. Wikipedia; and

g) any other websites that allow individual users or companies to use simple publishing tools, (together called **social media**)

7.2 Use of Social Media as part of your role

If you are required by the School to participate in Social Media sites as part of your role with the School you should ensure that you clearly understand what is required of you.

- Always exercise responsibility and judgment in any material you post on Social Media sites
- Essentially the rules that apply to you when you are interacting face to face with people as a representative of the School will apply to your actions on Social Media – including all School policies.
- Similarly the normal authorisation and approval process in relation to any content that you are posting will also apply.
- At SJIS, Marketing Dept is authorised to manage and use school social network as part of its enrolment activity. You can't post without permission.

- Be polite and respectful of the opinions of others at all times and refrain from posting any comments which harshly criticise or undermine posts made by others.
- Be careful of what you say about others and do not post comments which may be viewed as denigrating or insulting including to other schools
- Especially careful when posting photos.

7.3 Personal use of Social Media

7.3.1 Use of Social Media

The School understands that you use various Social Media for personal reasons on your own computers or other electronic communication technologies or on School Systems if you have been authorised to do so.

Generally what you do on your own time is your own business. However, information you provide, and statements you make, on Social Media sites may impact the workplace and have significant consequences. This material may be read by others in the School community or the public at large. Once information is published online, it is essentially part of a permanent record, even if you 'remove/delete' it later or attempt to make it anonymous.

When using any Social Media you are responsible for your words and actions.

It is your responsibility to ensure that your posts are appropriate. Use your judgment and common sense, and if there is any doubt, do not post.

When using any Social Media you must not:

a) invite students to join your personal social networking site or accept a students' invitation to join theirs;

b) communicate with students on social networking sites;

c) post photos of students or parents on social networking sites;

d) use the School's logo or create School branded accounts which could be interpreted as representing the School;

e) contribute anything which would bring you or the School into disrepute – for example an offensive blog or photo;

f) engage in any conduct that would not be acceptable in the workplace - for example:

i. making any adverse, offensive or derogatory statements about other employees or contractors, students, parents or Management of the School; or

ii. engaging in unlawful discrimination, harassment or bullying of other employees or contractors, students, parents or Management of the School; and

g) disclose any confidential information about the School, including information about other

The above requirements apply regardless of whether you have restricted access to your personal site to selected persons only.

You should also avoid identifying or discussing co-workers (and school officials as students/parents) or posting photographs that include co-workers unless you have obtained their permission first.

7.3.2 Expressing your personal views

It can be difficult to draw a line between your personal and professional life when using Social Media. Even when you are talking as an individual, people may perceive you to be talking on behalf of the School. By identifying yourself as a School employee or contractor, you are creating perceptions about your expertise and about the School. Accordingly you need to be careful that all content associated with you does not conflict with School policies and your obligations as an employee or contractor.

Just because conduct is outside work or you have not clearly identified yourself as a School employee or contractor, it may nonetheless be in breach of your obligations to the School as an employee or contractor, whether on Social Media or otherwise. You should exercise caution and common sense on that basis.

This policy is not designed to infringe upon your personal interaction or online conversations where you are clearly speaking as an individual with no reference to the School or your position as a School employee, provided you are otherwise complying with the School's policies and your obligations as an employee or contractor.

7.3.3 Time spent on Social Media

You may access Social Media sites during authorised breaks using your own computers or other electronic communication technologies or on School Systems if you have been authorised to do so. Excessive use of Social Media during work time for personal reasons may result in disciplinary action.

7.3.4 Personal liability

Please bear in mind that information you provide, and statements you make, on Social Media could have significant consequences for you personally, for example:

a) making statements about an individual may constitute defamation (in which case you may be personally liable under applicable legislation to the person about whom you make the statement);

b) making statements may constitute unlawful discrimination, harassment or bullying (in which case you may be personally liable under applicable legislation);

c) making statements about the School, its business, parents or students, may constitute a breach of your obligation not to disclose confidential information and your obligation not to make public statements about or on the School's behalf without express authority; and

d) using other persons' material, text, photographs, music, logos and trademarks may breach copyright laws.

7.3.5 Please take care

The terms and prescribed conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of Social Media. You are encouraged to act with caution and to take into account the underlying principles of this Policy. If you feel unsure about what to do in particular circumstances, you should contact the Principal, GM or Heads.

8. Intellectual Property

When distributing information over the School Systems or to third parties outside the School, you must ensure that you and the School have the right to do so and that you are not violating the intellectual property rights of any third party.

This applies in the same way when copying information or downloading software. In particular, copyright law may apply to the information you intend to distribute or copy, and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through e-mail without specific authorisation to do so. This material may be able to be used and copied in a limited way for research or educational purposes.

If you are not sure if you are allowed to distribute or copy certain information, contact the Principal, GM or Heads.

9. Privacy

In the course of carrying out your duties as an employee or contractor of the School, you may have access to or handle personal information relating to others, including other co-workers, suppliers and contractors. E-mail should not be used to disclose personal information of another person except in accordance with the School's Privacy Statement or with authorisation from the HR Department.

In order to comply with the School's obligations under privacy law, you are encouraged to use the blind copy option when sending e-mails to multiple recipients, because disclosure of those persons' e-mail addresses may impinge upon their privacy.

10. General

10.1. Please take care

The terms and prescribed conduct described in this Code are not intended to be exhaustive, nor do they anticipate every possible use of School Systems. You are encouraged to act with caution and to take into account the underlying principles of this Code. If you feel unsure about what to do in particular circumstances, you should contact the Principal, GM or Heads.

10.2. This Code is a direction

This Code sets out the rules which must be complied with when using School Systems. This Code is a direction to you by the School as an employee or contractor of the School. You must comply with this Code. If you do not comply with this Code, the School may take disciplinary action, up to and including termination of your employment or engagement.

10.3. User acceptance

Use of School Systems indicates agreement to comply with this code.

Staff Agreement 2024
Acceptable Use of Digital Technology and ICT Policy

All staff must carefully read this ICT policy and agreement prior to signing it. Any questions should be addressed to the school management and clarification obtained before the agreement is signed.

Staff Safe and Responsible Behaviour:
When I use school digital technologies;

1. Use for educational purposes
2. Always Carefully use and store safely
3. Safely use digital technologies to protect personal information
4. Respect myself and others by thinking about what I share online/social network
5. Understand that I accept responsibility for any costs associated with the repair or replacement if caused by any negligent act.
6. Return all devices when terminate

The device I was provided:

Chromebook # and charging code	**Serial number:**
iPad # Pen # and charging code	**Serial number:**
	Received Date

I have read the Agreement of digital technology and ICT Policy 2024.

Name: _____ **Signature :** _____

Date : _____

PLEASE SIGN AND RETURN THIS PAGE TO HEAD of the Division