Tech-Related Policies & Information

Table of Contents

NSW School of Languages Cyberbullying Policy

1. Purpose statement

In accordance with the school's **Anti-Bullying Policy** and the **National Safe Schools Framework**, NSW School of Languages seeks to:

- affirm the rights of all members of the school community to feel safe and be safe at school;
- acknowledge that being safe and supported at school is essential for student wellbeing and effective learning;
- accept responsibility for developing and sustaining safe and supportive learning and teaching communities which also fulfill the school's child protection responsibilities;
- encourage the active participation of all school community members in developing and maintaining a safe school community where diversity is valued;
- actively support young people to develop understanding and skills to keep themselves and others safe;
- commit to developing a safe school community through a whole-school and evidence-based approach.

2. Definition of cyberbullying

Cyberbullying is commonly defined as the use of information and communication technologies to support repeated and deliberate hostile behaviour intended to harm others. It is sometimes used as an extension to other forms of bullying, and can result in the target of bullying experiencing social, psychological and academic difficulties.

Cyberbullying can be conducted in many ways, using different media including:

- the sending of abusive texts, emails or instant messages;
- taking and sharing unflattering or private images, including naked or sexual images;
- posting unkind messages or inappropriate images on social networking sites;
- excluding individuals from online chats or other communication;
- assuming the identity of the victim online and repeatedly representing them in a negative manner or manner that may damage their relationship with others;
- for no strategic reason, attacking players in online gaming.

Like other forms of bullying such as verbal abuse, social exclusion and physical aggression, cyberbullying has the potential to result in the target of bullying developing social, psychological and educational issues.

While cyberbullying is similar to real life bullying it also differs in the following ways:

- it can be difficult to escape and can be invasive — it can occur 24/7 and a person can be targeted while at home;
- it can involve harmful material being widely and rapidly disseminated to a large audience, for example, rumours and images can be posted on public forums or sent to many people at once;
- it can provide the bully with a sense of relative anonymity and distance from the victim, so there is a disengagement of consequences.

3. Responding to incidents (students, parents, teachers, Deputy Principal)

When dealing with incidents of cyberbullying concerning NSW School of Languages

students: NSW School of Languages **students** should:

- ignore it – don't respond to the bully. If the bully does not get a response, they may get bored and go away;
- block the bully as this will stop the student from seeing messages or texts from them;
- save the evidence as it can be useful in tracking the bully down. Save all texts, emails, online conversations or voicemails as evidence;
- report the abuse to their NSW School of Languages teacher immediately (whether the bully is from NSW School of Languages or not);
- consult the school's **Cybersafety Guide for Families** for tips on preventing cyberbullying and managing cybersafety in general;

Parents of NSW School of Languages students should:

- notify their child's NSW School of Languages teacher as well as the relevant person in their child's home school, if they observe changed behaviours in their child or have concerns about possible incidents of cyberbullying involving other students (whether the bully is from NSW School of Languages or not);
- ensure their child reports any incident involving cyberbullying by another NSW School of Languages student to their NSW School of Languages teacher immediately or any incident involving cyberullying by another student in their home school to the relevant person in that home school;
- consult the school's **Cybersafety Guide for Families** for tips on preventing cyberbullying and managing cybersafety in general;
- contact your local Police if there is a threat to your child's safety. In life-threatening and time-critical situations call Triple Zero (000).

NSW School of Languages **teachers** should:

- be observant of changes in their students' behaviour;
- encourage students to be respectful of one another and to be sensible digital citizens e.g. by referring them to the websites listed in this policy and by consulting the school's **Cybersafety Guide for Families**.
- ensure their students feel they can approach them to discuss any matter, including possible incidents of cyberbullying by other students (whether the bully is from NSW School of Languages or not);
- not delete any evidence of cyberbullying when shown to them by a student, but rather save and confiscate the evidence;
- report the incident to the Deputy Principal.

The **Deputy Principal** should:

- fully investigate the incident including gathering all related evidence;
- contact the student's parents;
- contact the student's home school to notify them of any incident of cyberbullying involving that student (whether the bully is from NSW School of Languages or not);
- implement disciplinary procedures for the perpetrators if they are NSW School of Languages students, as per regular guidelines for dealing with incidents of bullying in **NSW School of Languages's Anti-Bullying Policy**.

Cyberbullying is a part of **NSW School of Languages's Anti-Bullying Policy**. If a cyberbullying incident occurs amongst NSW School of Languages students, it must be reported immediately and will be managed as per the procedures set out in **NSW School of Languages's Anti-Bullying Policy**.

4. Links to relevant websites & documents

- NSW School of Languages Links & Resources
  - ⇒ Cybersmart Guide for Families
  - ⇒ Cybersafety Online Exercise for Students
  - ⇒ NSW School of Languages Acceptable Use of Digital Technologies Agreement
  - ⇒ NSW School of Languages Anti-Bullying Policy (in progress)

- External Links & Resources
  - ⇒ NSW DEC Schools AtoZ Technology Guide (website - Australian)
  - ⇒ NSW DEC Cyberbullying Advice for Parents (Downloadable PDF – Australian)
  - ⇒ ACMA Cybersmart YouTube Channel (website - Australian)
  - ⇒ ACMA Cybersafety Guide for Parents (online video - Australian)
  - ⇒ ACMA Cybersafety Guide for Parents (Downloadable PDF - Australian)
  - ⇒ ACMA Cybersmart Guide for Teens (website - Australian)
  - ⇒ Kids Helpline Cyberbullying Information (website - Australian)
  - ⇒ Stay Smart Online (website - Australian)
  - ⇒ Bullying No Way! (website - Australian)
  - ⇒ Stop Cyberbullying (website - USA)
  - ⇒ Cyberbullying: A whole school community issue (Downloadable PDF - UK)
  - ⇒ ThinkUKnow (website - UK)

NSW School of Languages
Bring Your Own Device (BYOD) Policy

Requirements for NSW School of Languages that allow staff and students to use personal mobile electronic devices at school, with the capability of connecting to the department's wi-fi network.

1. **Objectives - Policy statement**
   - 1.1 NSW School of Languages allows staff and students to bring their own personal mobile electronic devices to school for the purpose of teaching and learning
   - 1.2 School-developed guidelines and procedures for BYOD are available to staff, students, parents and caregivers
   - 1.3 The use of personal mobile devices at school will assist to deepen learning.

2. **Audience and applicability**
   - 2.1 NSW School of Languages staff, parents, caregivers and students.

3. **Context**
   - 3.1 The increasing availability of personal mobile devices has accelerated the demand for new models of learning.
   - 3.2 NSW School of Languages is in a position to harness staff and students' connection to their own personal mobile devices for the purpose of developing 21st century learning skills and for fostering digital literacy, fluency and citizenship in a safe environment.

4. **Responsibilities and delegations**
   - 4.1 **The TSU**
     - 4.1.1 The TSU (Tech Support Unit) at NSW School of Languages is responsible for the surveillance and monitoring of its computer systems to ensure the ongoing confidentiality, integrity and availability of services.
   - 4.2 **The Head Teacher E-Learning & Technology**
     - 4.2.1 The Head Teacher E-Learning & Technology at NSW School of Languages is responsible for developing and implementing the school's BYOD policy.
   - 4.3 **The staff member/student**
     - 4.3.1 The staff member or student is responsible for abiding by the school's policy and the department's Online Communication-Acceptable Usage for School Students.

5. **Monitoring, evaluation and reporting requirements**
   - 5.1 NSW School of Languages will update this policy as required.

NSW School of Languages
Bring Your Own Device (BYOD) Device Requirements

Wireless connectivity:

The department's Wi-Fi network installed in high schools operates on the 802.11n 5Ghz standard. Devices that do not support this standard will not be able to connect. This may be advertised as "Dual Band Wireless", "802.11abgn", "802.11agn", "802.11ac" or "Gigabit Wireless".

Note: Devices marketed as "802.11bgn" probably do **not** support the required standard.

Form Factor:

Laptop, tablet device or convertible device. A tablet device *must have a physical keyboard attachment with separate keys* for A – Z and 0 – 9.

Physical Dimensions:

- Minimum Screen Size: 9.7" or 24.5cm
- Maximum Screen Size: 13.3" or 33.5cm

Operating system:

- Microsoft Windows 7 or newer
- Apple MacOS X 10.6 or newer
- Apple iOS 6 or newer
- Microsoft Windows RT

Software and apps:

School-based requirements. All software and apps should be fully updated.

Battery life:

Advertised battery life of six hours.

Memory and RAM:

A minimum specification of 16 GB storage and 2 GB RAM to process and store data effectively.

Hardware features:

Camera and microphone.

Ergonomics:

Reasonable sized screen and a sturdy keyboard to enable continuous use throughout the day.

Other considerations:

- Maximum weight: 2kg
- Minimum RAM (laptops): 4GB
- Disk configuration (laptops): Solid State disk

Accessories:

- Carry case: Supply a carry case or skin to protect the device.
- Insurance and warranty: Be aware of the terms of insurance policies/warranties for the device. The school will not accept responsibility for loss or breakage.
- Back-up storage: Consider a portable hard drive as an appropriate source of back-up storage for essential documents.

NSW School of Languages
Bring Your Own Device (BYOD) Student Responsibilities

Operating system and anti-virus:

Students must ensure they have a legal and licensed version of a supported operating system and of software. If applicable, students' devices must be equipped with anti-virus software.

NSW Department of Education and Communities' Wi-Fi network connection only:

Student devices may only connect to the department's Wi-Fi network while at school. There is no cost for this service.

Battery life and charging:

Students must ensure they bring their device to school fully charged for the entire school day. No charging equipment will be supplied by the school.

Theft and damage:

Students are responsible for securing and protecting their devices at school. Any loss or damage to a device is not the responsibility of the school or the Department.

Confiscation:

Students' devices may be confiscated if the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement.

Maintenance and support:

Students are solely responsible for the maintenance and upkeep of their devices.

Ergonomics:

Students should ensure they are comfortable using their device during the school day particularly in relation to screen size, sturdy keyboard, etc.

Data back-up:

Students are responsible for backing-up their own data and should ensure this is done regularly.

Insurance/warranty:

Students and their parents/caregivers are responsible for arranging their own insurance and should be aware of the warranty conditions for the device.

NSW DEC Online Communication Services: Acceptable Use for School Students Policy

This document defines the policy for school students of the NSW Department of Education and Communities for the appropriate and acceptable use of internet and online communication services provided by the Department.

1. Objectives - Policy statement

1.1 The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Today's students are exposed to online communication tools and the internet in their community. They have the right to expect secure access to these services as part of their learning experiences with the NSW Department of Education and Communities.

1.2 Use of the internet and online communication services provided by the NSW Department of Education and Communities is intended for research and learning and communication between students and staff. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

1.3 Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

1.4 Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to their supervisors.

1.5 Students who use the internet and online communication services provided by the NSW Department of Education and Communities must abide by the Department's conditions of acceptable usage. They should be made aware of the acceptable usage policy each time they log on.

1.6 Students should be aware that a breach of this policy may result in disciplinary action in line with their school's discipline policy.

2. Audience and applicability

2.1 This policy applies to all school students located at NSW public schools who access internet and online communication services within the NSW Department of Education and Communities network and from any external location.

3. Context

3.1 This policy document takes account of the Memorandum Student Access to the Internet of 18 July 1997 and the Memorandum DN/04/00215 – Review by Schools of their Student Access to the Internet Policies.

3.2 This policy document should be read as consistent with school discipline, child protection, anti-discrimination and anti-racism policies:

4. Responsibilities and delegations

4.1 Access and Security

4.1.1 Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- ensure that communication through internet and online communication services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their personal e-learning account.

- log off at the end of each session to ensure that nobody else can use their e-learning account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
  - a message that was sent to them in confidence.
  - a computer virus or attachment that is capable of damaging recipients' computers.
  - chain letters and hoax emails.
  - spam, e.g. unsolicited advertising material.
- never send or publish:
  - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
  - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
  - sexually explicit or sexually suggestive material or correspondence.
  - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and internet and online communication services is generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks of the NSW Department of Education and Communities.
- ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

4.1.1 Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.2 Intellectual Property and Copyright

4.1.1 Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.

- ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

4.2 Misuse and Breaches of Acceptable Usage

4.1.1 Students will be aware that:

- they are held responsible for their actions while using internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.
- the misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, evaluation and reporting requirements

5.1 Students will report:

- any internet site accessed that is considered inappropriate.
- any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education and Communities.

5.2 Students should be aware that:

- their emails are archived and their web browsing is logged. The records are kept for two years.
- the email archive and web browsing logs are considered official documents.
- they need to be careful about putting their personal or sensitive information in emails or on websites.
- these records may be used in investigations, court proceedings or for other legal reasons.

6. Contact

6.1 Director, NSW Curriculum and Learning Innovation Centre, (02) 9715 8150.