LAUDE SAN PEDRO INTERNATIONAL COLLEGE

E Safety Policy

2025

Contact details		
Principal	Mandy Palmer	m.palmer@laudesanpedro.com
Assistant Principal of Safety and Wellbeing	Nicky de Comarmond	n.decomarmond@laudesanpedro.com
EYFS & Primary	Arancha Barrasa	a.barrasa@laudesanpedro.com
Secondary	Joe Short	j.short@laudesanpedro.com
ISP Regional Managing Director	Miguel Ángel Garrán	mgarran@ispschools.com

1.0 Introduction

At Laude San Pedro we want all members of our community to have a shared understanding of our vision, values, standards, policies and procedures so that we can all work towards creating a positive and ambitious learning environment for the pupils in our care:

VIsion

"Safe, Happy, Learning"

Missions

We inspire students to become motivated, respectful learners in our inclusive and vibrant international school community. We empower our students to reach their individual potential through building positive relationships in a safe, happy and nurturing environment.

Core values

Resilience
Empathy
Aspiration
Courage
Honesty

2.0 Rationale

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children, young people and staff is paramount when using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety and that our codes of conduct are adhered to
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices
- establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using our network and devices

- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- all children, regardless of age, disability, gender reassignment, race religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse

3.0 Role and Responsibilities

All staff

We will seek to keep children and young people safe by:

- modelling responsible use of technology and signing their agreement of the Acceptable Use policy (see Appendix 1)
- delivering e-safety lessons and reinforcing good practices (EYFS, Primary and relevant specialist teachers in Secondary)
- reporting e-safety concerns promptly
- providing clear and specific directions to staff and volunteers on how to behave online through our Staff Code of Conduct
- supporting and encouraging the children to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents or carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- reviewing and updating the security of our information systems regularly
- ensuring that usernames, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the school.

Staff are vigilant during use of websites/technology, and will monitor for potential risks including:

- Harassment or online bullying ("cyberbullying") on the part of the student or others'
- Posting information about themselves that: a) could be used to embarrass or manipulate them; b) could cause psychological harm; c) could be used

by criminals to steal their identity or property or – though very rare – determine their physical location to cause physical harm
- Damage to reputation or future prospects because of young people's own behaviour or that of their peers – unkind or angry posts, compromising photos or videos, or group conflict depicted in text and imagery
- Spending too much time online, losing a sense of balance in their activities
- Exposure to inappropriate content
- Potential for inappropriate contact with adults (parents/guardians need to ensure that social networking does not lead to offline contact unapproved by them and other caring adults in their children's lives).
- Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE) which can start on Social Media.

Parents/Carers

We ask that all families:

- support the school's e-safety policy and discuss safe internet use at home
- monitor their child's use of online platforms and apps
- report e-safety concerns to the school

Students

All students are expected to:

- use technology responsibly and respectfully
- maintain good online behaviour and not to do or participate in anything that is illegal or criminal or that involves a violation of the school's rules
- act with caution and discretion on the internet, and to adopt and maintain at all times an attitude of caution
- think before writing, publishing and sharing something, considering the importance and significance if this is then shared more widely
- avoid posting comments or images that may annoy, anger, harm or hurt other people
- avoid using any kind of language that may be considered blasphemous, profane, obscene or threatening
- keep their passwords secret and secure by not sharing them with anyone other than their parents or legal guardians. If someone appropriates their identity on the internet without their knowledge, they may be held responsible
- use the school email account exclusively for academic purposes, understanding that it is a work tool; the school reserves the right to remove the email account in cases where inappropriate or improper use has been detected and is deemed necessary
- act with absolute caution when participating in online games, opening emails where there could be suspicion, participating in surveys and invitations from unknown sources, avoid pages that ask for money or credit card information, maintaining the integrity of the school and protecting its information
- not enter unreliable web pages
- not chatting, sending or consulting messages, playing and watching videos unless directly asked to do so, downloading music, commenting on blogs or forums, playing or participating in online games, entering social

networks, participating in contests, creating events, contracting services or purchasing products online
- deliver and show the device to the teacher whenever they consider it appropriate or where there is a concern of misuse
- report any inappropriate content or behaviour to a trusted adult
- follow the school's rules for safe internet use
    - Never arrange to meet anyone you have met on the web
    - Never give out personal information e.g., telephone numbers, address, photos
    - If you come across anything on the web that is inappropriate/offensive, tell an adult
    - Never use your real name – always a nickname
    - Keep your password a secret from others – only share passwords with parents/carers so they can support you
    - If you receive a nasty message or picture, report it to an adult, block and report it to the site you are on
    - Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos
    - Only use a webcam with people you know and have met face to face

The use of social networking sites is not permitted in school, on school equipment.

4.0 Use of technologies

Whether using school equipment or their own device (as is currently the case in Sixth Form), users shall not visit internet sites, make, post, download, pass on, remark or comment on content that relates to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting religious hatred
- promoting illegal acts
- weapons
- display any other information that may be offensive to other students, staff, visitors, or any member of the public
- use any other users accounts nor amend or delete any of the accounts, files or passwords
- install or attempt to install programmes of any type

It is important that students understand

- they must avoid using the school's logo, uniform, symbols and other associated images of Laude International College in their personal social network accounts, without the express authorisation of the Principal
- they must act correctly and cautiously in the publication of photos and images when wearing the school uniform. In this sense, Laude International College reserves the right to demand the removal from the internet any images or content related to the school and published without the consent of the Principal
- it is considered extremely serious behaviour by the student if they make jokes, mockery, hurtful, malicious or offensive comments on the internet

and social networks about other students, parents, families, tutors, teachers, administrative and service staff or management team
- that the law punishes the manufacture or possession of tools, materials, instruments, substances, machines or devices intended to commit crimes and, more specifically, those intended for the falsification of official or private documents with the intent to deceive

In any instance where inappropriate content is suspected or observed, staff members are to apply the school rules as applicable. Content used to bully others will be taken very seriously as per the Behaviour and Anti-Bullying Policy.

If the material is deemed to be serious, a device may be confiscated and retained as evidence (of a criminal offence or a breach of school rules). Examples of illegal activity that may require police intervention would include.

- Child sexual abuse and images (including images of one child held by another child)
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Recordings of criminal activity as a witness (this includes child on child abuse, including 'upskirting')
- The use of weapons to injure someone

If students appear to have been 'sexting' each other or someone outside of school, staff will immediately inform the DSL who will conduct a full investigation. This may result in internal sanctioning or referral to the Police or Children's Services if one or more party are at risk of harm.

NB – Sexting means 'sending sexually explicit messages and/or suggestive images, such as nudes. While the name suggests that this is done via text messages, these types of messages can be sent via any messaging service, including emails and social media sites/apps. It is illegal for a child aged under 18 to take a nude photo of themselves or a friend, as well as distributing them.

5.0 Monitoring

The School has appropriate filtering and monitoring systems in place using **SMOOTHWALL** to protect students on the Internet (including email text messaging and social media sites) when connected to the School's network. The system is checked termly to ensure that it is working appropriately.

Devices equipped with a mobile data subscription can, however, provide students with unlimited and unrestricted access to the internet. Since the School cannot put adequate protection for the students in place in these cases, students are not allowed to use these devices to connect to the Internet including accessing email, text messages or social media sites when in the School's care.

In certain circumstances, such as for monitoring a medical condition, a student may be given permission to use their own mobile device to connect to the Internet using the School's network. Permission to do so must be sought and given in advance.

- The School rules about the use of mobile electronic devices are set out in the Acceptable Use Policy
- The use of mobile electronic devices by staff is covered in the Staff Code of Conduct. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.
- The School's policies apply to the use of Technology by staff and students whether on or off School premises and appropriate action will be taken where such use affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

6.0 Cyber Bullying and threats

Cyberbullying or bullying through the Internet is defined as the use and dissemination of information, real or fictitious, with harmful or defamatory intent and in electronic format.

Such dissemination can be done through different digital media such as email, instant messaging, forums, chats, social networks, text messaging through mobile devices or the publication of videos or photographs on electronic platforms for content dissemination.
This form of bullying or harassment can manifest itself in many different ways. In this regard, students have the duty to:

- maintain a behaviour and attitude of vigilance and responsibility in the defense and protection of their personal data and those of their classmates
- not engage in cyber bullying behaviour, and in the case of being affected by or having knowledge / facts about, must report it immediately to teachers
- denounce and not consent to acts of psychological or moral violence to other students on any forum, from the moment they become aware of it
- avoid at all times making jokes about behaviour that may be defined as bullying and cyberbullying
- avoid bullying, cheating, teasing, mocking, rejecting and any kind of discrimination, exclusion and/or harassment of other students with offensive comments on any forum
- not send, show or share any pictures or images of another classmate with the intention of making fun with their friends
- not to post comments, photos or videos that may damage the reputation, defame or hurt the feelings of another student
- not use offensive, threatening or intimidating messages or messages containing aggressive and foul language or vocabulary, and must also not use messages that, directly or indirectly, are insulting or imply harassment, exclusion or manipulation
- not share gossip or false rumours of a cruel nature or that are intended to damage the reputation of another student
- not record intimate content and compromising private images of another student

- not forwarding or circulating personal information about other students and/or their families to other students or people outside of the school
- not to respond to threats, insults, intimidating messages or provocations that are made on any forum. In this situation, the student should always bring it to the attention of their parents and teachers

Situations which are considered **aggravating factors**:

- threatening to publicise a matter
- threatening to disclose or share facts about another student's private life or relationships in cases where the person's reputation or personal interests may be affected if the threat is carried out
- coercion: a threat that seeks, by means of violence of any kind, to prevent a students from doing something lawful or in accordance with school rules, or to force a student the do something they don't want to do
- blackmail: threat with a condition, something that is demanded in exchange for not complying with it

It is slander to claim that another student has acted outside or contrary to the policy whilst knowing that they have never committed any offense against the policy.

Slander is any action or expression - humiliation, insult or offense - of a serious nature that injures the dignity of another student, undermines their reputation, or is an affront to their self-esteem

7.0 Infringements against privacy

Infringement or violation of the right to privacy can have legal consequences: the law prohibits accessing, seizing, using, modifying and altering the personal data and privacy of another individual to his or her detriment.

The secrecy of communications is a fundamental right of individuals and failure to respect it can lead to serious consequences. E-mail, instant messaging, chat conversations, sms, social networks, etc., are means of communication and, in case they are made privately, they are protected by law.

In this sense, the dissemination, disclosure or transfer to third parties of other people's data without consent, for example, with its publication on the Internet, can have legal repercussions, particularly serious if they concern a minor affected.

In relation to personal privacy, Article 18.4 of the Spanish Constitution guarantees the protection of personal data, so that they cannot be used without the informed consent of the owner and for specific purposes.

It is extremely important that students are aware of the extent to which their behaviour may or may not be appropriate and, above all, that they know and value the importance of respecting the privacy of others and the possible consequences of acting otherwise.

- When recording and/or publishing images and photographs featuring other students, it is the student's duty to do so with the consent and permission of the other students.
- It is the student's duty to refrain from uploading, posting or linking any document or image - photographs, videos, web pages, audio files, forums, groups, chats, etc., that may be a cause and reason for damage, discredit or present or future harm to the privacy of another student.
- It is the student's duty to avoid reading another student's email without permission, as well as entering another student's computer or system without permission, which is an invasion of another student's privacy.

8.0 Curriculum

As part of the ICT/Computing and PSHE curriculum, all students will undertake awareness lessons in E-Safety. This is further reinforced in all other areas of the curriculum, especially when working with technology. The key messages from these lessons are:

- The dangers of using the internet/apps both at home and at school
- What to do if they come across inappropriate/offensive text or images
- How to stay safe when communicating online
- How to take appropriate action when things go wrong
- How to stay safe when using Social Networking sites
- How to stay safe in chat rooms/discussion forums
- What to do if they are a victim of cyberbullying
- The dangers and laws of 'sexting' and sharing inappropriate images/videos

9.0 Reporting

Staff, students and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures. Please also refer to **Appendix 2.**

Misuse by students

- Anyone who has any concern about the misuse of Technology by students should report it to the KS leader in the first instance, so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying. This applies to any misuse when off school premises also.
- Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy.

Misuse by staff

- Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy directly to the school Principal, so that it can be dealt with in accordance with the staff disciplinary procedures.
- If anyone has a safeguarding-related concern, they should report it immediately to the DSL so that it can be dealt with in accordance with the

procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding & Child Protection Policy.

Misuse by any user

- Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Head of Section or the Principal.
- The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

10.0 Responding to misuse or online abuse

For any misuse or online abuse, steps will be followed as outlined in the School's behaviour policy or anti bullying policy as relevant.

All cases of misuse and online abuse are taken seriously to protect the child.

The following policies, procedures and resource materials are also relevant to the School's online safety practices:

- Anti-Bullying Policy
- Acceptable use policy agreement
- Safeguarding and Child Protection Policy
- Mobile phone and camera policy

11.0 Interpretation

Any enquiries regarding the application of this policy should be addressed to the Director of Operations at:
33 Cavendish Square,
London,
W1G 0PW

12.0 Policy Tracker

Date Created	Author	Revision due date
February 2025	Assistant Head: Safety and Wellbeing	February 2026

Appendix 1

LAUDE
SAN PEDRO
INTERNATIONAL COLLEGE

ACCEPTABLE USE POLICY - STAFF AGREEMENT This policy covers use of digital technologies in school / issued for school use: i.e. email, internet, intranet and network resources, learning platform, software, equipment and systems.	
Name:	
School issued email account:	
Please sign below where indicated to confirm that you have read and understood this document.	

1. I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Principal and ISP.
2. I will not reveal my password(s) to anyone.
3. I will not allow unauthorized individuals to access email / Internet / intranet / network.
4. I will not engage in any online activity that may compromise my professional responsibilities.
5. I will only use the approved, secure email system(s) for any school business.
6. I will only use the approved school communication systems with pupils or parents / carers, and only communicate with them on appropriate school business.
7. I will not browse, download or send material that could be considered offensive or illegal.
8. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach.
9. I will not download any software or resources from the Internet that can compromise the network or are not adequately licensed.
10. I will not connect a personal computer or other device, to the network / Internet unless authorized to do so by the Principal.
11. I will not use personal digital cameras or phones for taking and transferring images of pupils or staff at work and will not store images on personal devices.
12. I will use the school's Learning Platform in accordance with School policy.
13. I will ensure that any private social networking sites / blogs / vlogs / podcasts / written publications etc that I create or actively contribute to are not confused with my professional role, and I will seek permission from the School Principal if I intend to contribute to any such areas.

14. I agree and accept that any phone, computer or laptop or other electronic device loaned to me by the school, is provided solely to support my profession and can be audited without notification including the search history and files

15. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

16. I understand that the school's data protection policy requires that any information seen by me regarding staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

17. I understand that all Internet usage / and network usage can be logged, and this information could be made available to my manager on request.

18. I understand that the School has ownership of any Intellectual Property Rights when I create original work in the course of employment (whether or not during working hours or using the Schools premises or resources, and whether or not recorded in material form).

19. When my contract ends, I agree to the transfer of all files on the accounts provided by school as well as any hard copies.

20. I understand that failure to comply with this agreement could lead to disciplinary action.

21. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school Acceptable Use Policy.

22. I agree to abide by all the points above.

Signature:

Print Name:

Date:

Appendix 2

What to do if a cyber bullying incident occurs:

If a bullying incident directed at a child occurs using email or social media technology, either inside or outside of school time, teachers should:

1. Advise the child not to respond to the message
2. Refer through My Concern as a safeguarding concern
3. Investigate, document and secure all evidence in line with policies
4. Notify parents of the children involved
5. Consider informing the police depending on the severity or repetitious nature of offence
6. Inform the School Safeguarding officer
7. Apply appropriate sanctions

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform the site administrators and / or ISP and request the comments be removed if the site is administered externally
2. Secure and preserve any evidence
3. Endeavour to trace the origin and inform police as appropriate
4. Report on My Concern as a safeguarding concern

Children and staff should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear, even if they have initially responded to the abuse.