



ONLINE SAFETY AND SAFEGUARDING POLICY

1. Purpose and scope

Tecnis Academy is committed to providing a safe, respectful and secure online learning environment. This policy sets out the standards and arrangements that apply to virtual teaching, digital platforms, online communication, recordings and the use of technology in connection with Tecnis Academy.

This policy applies to all Tecnis Academy employees, tutors, teaching assistants, administrators, contractors, volunteers and other adults working with or supporting students; all students; and all parents, carers and other adults who support a student's participation in Tecnis online learning. It applies to Tecnis-approved virtual classroom platforms, Google Classroom, Google Drive, Tecnis accounts, online communications, lesson recordings and other digital systems used for teaching.

This policy is intended for students, parents/carers, staff and other members of the Tecnis community. Detailed internal safeguarding and incident-management procedures are maintained separately and are not reproduced in full in this public-facing policy.

2. Safeguarding and online safety

Tecnis Academy takes safeguarding seriously. The safety and welfare of children and young people is a priority in all online teaching arrangements, and concerns arising during virtual lessons will not be ignored or neglected.

All staff and tutors have a responsibility to act promptly when they become aware of a safeguarding concern. Concerns must be reported to the Designated Safeguarding Lead (DSL) or the relevant safeguarding lead without delay. The DSL/safeguarding team will determine the appropriate action and, where necessary, will review relevant information such as lesson recordings, platform records or communications and contact parents/carers or appropriate external agencies.

Where a student or another person is believed to be in immediate danger, the appropriate emergency services should be contacted without delay. Staff should not undertake their own investigation into a safeguarding concern; they should report the concern and follow Tecnis's safeguarding procedures.

The same expectations of professional conduct, safeguarding, respect and confidentiality apply online as they do in other educational settings.

3. Responsibilities

3.1 Senior leadership

Senior leadership has overall responsibility for ensuring that appropriate online-safety and safeguarding arrangements are in place, adequately resourced, implemented and reviewed. Online safety will be considered alongside Tecnis's wider safeguarding, dataprotection, risk-management and staff-conduct arrangements.

3.2 Designated Safeguarding Lead

The DSL is the principal safeguarding point of contact for online-safety concerns. The DSL oversees safeguarding referrals and records, provides advice to staff, determines whether further action or referral is required, and works with relevant staff and technical leads where online systems, recordings or digital evidence are relevant to a concern.

3.3 Tutors and staff

- Use only Tecnis-approved accounts, platforms and communication channels for teaching and student contact.
- Maintain appropriate professional boundaries and actively supervise live online lessons.
- Use available classroom controls appropriately and report safeguarding or serious online-safety concerns promptly to the DSL or relevant safeguarding lead.
- Treat student information and recordings as confidential and use approved systems for storing or sharing them.
- Complete required safeguarding and online-safety training and follow Tecnis policies and procedures.

3.4 Students

- Use Tecnis background and platforms responsibly and follow tutor instructions.
- Treat tutors and other students with respect and do not bully, threaten, discriminate against or harass others.
- Do not share passwords, lesson links, recordings, personal information or another person's images without permission.
- Report anything that makes them feel unsafe, uncomfortable or concerned to a tutor, parent/carers or Tecnis Academy to admissions@tecnisacademy.com.

3.5 Parents and carers

- Support students to follow Tecnis online-safety expectations and use learning platforms appropriately.
 - Take reasonable steps to prevent unauthorised people from joining lessons or accessing lesson links and recordings.
 - Do not record, photograph, screenshot or redistribute lessons or other students' information without Tecnis authorisation.
-
- Raise safeguarding, cyberbullying, inappropriate-contact, privacy or security concerns with Tecnis promptly.

4. Virtual classroom standards

Tecnis Academy's virtual classrooms are supervised educational environments. Only authorised participants should attend a lesson. Lesson links, passwords and joining information must be kept confidential and must not be shared publicly or with unauthorised persons.

Where platform functionality allows, Tecnis may use measures such as authenticated accounts, passcodes, waiting rooms/lobbies and participant controls. Tutors will check participants and may remove or block an unauthorised participant where necessary.

Tutors will maintain active supervision of lessons and will use appropriate controls over microphones, chat and screen-sharing. Students are expected to follow reasonable tutor instructions concerning these functions.

Students should use a suitable learning environment and should take reasonable care not to display private information, documents, addresses, family information or other sensitive material on camera or through screen-sharing. Tecnis recognises that students may participate from home and will not require unnecessary disclosure of private areas of the home.

Chat, audio, video and screen-sharing must be used for appropriate educational purposes. Offensive, threatening, sexualised, discriminatory, abusive or otherwise inappropriate material or behaviour is not permitted.

5. Recording and use of online lessons

Tecnis currently records virtual classes so that students can catch up or review lessons. Recordings are made available through Google Classroom and stored within Google Drive.

- Recordings are normally retained for 12 months and then deleted in accordance with Tecnis's retention arrangements.
- Recordings are used for educational purposes, quality assurance and safeguarding.
- Access is restricted to authorised users and must be through approved Tecnis systems.
- Recordings must not be downloaded, copied to personal storage, published or redistributed without authorisation.
- Where a recording is relevant to a safeguarding concern, complaint or legal requirement, Tecnis may retain it for longer where necessary and lawful.
- Students and parents/carers should not make their own recordings, screenshots or photographs of lessons involving other students unless Tecnis has expressly authorised this.

Tecnis's Privacy Policy provides further information about the collection, use, storage and retention of personal information.

6. Communication and professional boundaries

Tutors must maintain professional boundaries in all online interactions with students. Communication outside live lessons must take place through Tecnis-approved professional accounts and channels and should be limited to legitimate educational or safeguarding purposes.

Tutors must not use personal social-media accounts, personal messaging applications or private gaming accounts to communicate with students, and must not ask students to connect with or follow personal social-media accounts. Personal phone numbers should not be exchanged except where specifically authorised for a legitimate operational or safeguarding reason.

If a student contacts a tutor through a personal account, the tutor should not continue the private conversation. The student should be directed to an approved Tecnis communication channel and any concerning or safeguarding-related content should be reported to the DSL.

7. Cyberbullying, inappropriate behaviour and personal information

Bullying and harassment are not acceptable in Tecnis's online learning environment. This includes abusive or threatening messages, discriminatory language, humiliation, impersonation, exclusion, spreading rumours, sexualised comments, deliberate disruption and other behaviour intended to harm or intimidate another person.

Students must not share another person's personal information, passwords, photographs, location, medical information or other identifying information without appropriate permission. Sexual content, pornography, illegal material, intimate images or material that could place another person at risk must not be shared through Tecnis systems.

Tutors may restrict chat, microphones or screen-sharing, or remove a student from a lesson, where this is necessary to maintain a safe learning environment. Serious or repeated behaviour may result in further action under Tecnis's behaviour, safeguarding or disciplinary procedures.

8. Safeguarding concerns arising online

Safeguarding concerns may arise from what a tutor sees or hears during a lesson, including a student's behaviour, conversation, camera view, background, chat or screensharing. A concern may also arise through a recording, message, platform activity or report from a student or parent/carer.

All staff and tutors have a responsibility to act promptly when they become aware of a safeguarding concern. They must report the concern to the DSL or relevant safeguarding lead and provide any relevant factual information. Staff must not ignore a concern because it occurs online or because they are unsure whether it meets a particular threshold.

The DSL/safeguarding team will consider the information available and take the appropriate action in accordance with Tecnis's safeguarding procedures. This may include reviewing lesson recordings or other relevant information, speaking with the student, contacting parents/carers where appropriate, and making referrals to children's social care, the police or other agencies where required.

Where there is an immediate risk of serious harm, the appropriate emergency services should be contacted without delay. Detailed internal safeguarding procedures, including investigation, evidence handling and referral processes, are maintained separately.

9. Filtering, monitoring and home devices

Tecnis uses proportionate technical and organisational measures to support online safety on systems and devices within its control. This may include account controls, platform settings, filtering, monitoring, access logs and other security measures, subject to the functionality of the relevant technology.

Tecnis cannot routinely monitor everything a student does on a personal device or home network outside Tecnis-controlled systems. This includes private messages, personal social-media accounts, gaming platforms, other applications and the full traffic of a home broadband connection that Tecnis does not administer.

Parents/carers and students should therefore understand that Tecnis's online classroom controls do not constitute continuous monitoring of the home environment. Tecnis will nevertheless act on safeguarding concerns that come to its attention through lessons, recordings, approved systems, reports or disclosures.

10. Data protection, privacy and cybersecurity

Tecnis will process children's personal information in accordance with applicable dataprotection law and its Privacy Policy. Personal information will be accessed and shared only where necessary and through approved systems.

- Staff must not transfer student information or recordings to personal email, personal cloud storage or unauthorised devices.

- Screenshots should not be taken routinely. Where a screenshot or other digital evidence is necessary for safeguarding or an authorised investigation, it must be handled securely and only shared with those who need it.
- Staff and students must protect account passwords and authentication information and must not share accounts.
- Suspected account compromise, unauthorised access or a data-security incident must be reported promptly through Tecnis's reporting arrangements.
- Tecnis will take appropriate steps to protect recordings and other personal information from accidental loss, unauthorised access, alteration or disclosure.

11. Artificial intelligence

Tecnis recognises that artificial intelligence (AI) can support teaching and learning but also creates risks relating to privacy, inaccurate information, inappropriate content, academic integrity, manipulation and deepfakes.

- Staff must use only AI tools approved by Tecnis where Tecnis or student information is involved.
- Identifiable safeguarding information, sensitive personal data, passwords and confidential student information must not be entered into public AI tools unless the tool and use have been appropriately authorised.
- Students must follow tutor instructions regarding acceptable use of AI in learning and assessment.
- AI-generated or manipulated content that is abusive, sexualised, threatening, discriminatory or intended to humiliate another student is prohibited and may constitute a safeguarding concern.

12. Staff training and professional conduct

Staff and tutors who work with students online must receive appropriate safeguarding and online-safety induction before undertaking their duties independently. Training will cover safeguarding responsibilities, professional boundaries, virtual classroom controls, recording and privacy, cyberbullying, data protection, cybersecurity, AI-related risks and reporting routes.

Training will be refreshed at least annually and when significant changes to technology, safeguarding requirements or Tecnis's online-learning arrangements make additional training necessary.

13. Breaches and consequences

Tecnis will respond proportionately to breaches of this policy, taking account of the seriousness and circumstances of the incident, the student's age and needs, any safeguarding implications and whether the behaviour is repeated.

Depending on the circumstances, action may include restriction of online functions, removal from a lesson, parent/carer involvement, withdrawal of access to particular systems, formal behaviour or safeguarding action, staff management or disciplinary action, or referral to an external agency. Serious safeguarding concerns will be managed through Tecnis's safeguarding procedures rather than solely as behavioural matters.

14. Complaints, incidents and policy review

Concerns about online teaching, privacy, conduct or safety should be reported through the appropriate Tecnis reporting or complaints route. Safeguarding concerns should be referred directly to the DSL or relevant safeguarding lead.

Tecnis will review significant online-safety incidents and use learning from incidents, feedback, changes in technology and changes in relevant guidance to improve its arrangements.

This policy will be reviewed at least annually and sooner where there is a significant incident, a change to Tecnis's online teaching model or digital platforms, or a relevant change in legislation or guidance. The review will consider the effectiveness of safeguarding, recording, access control, filtering and monitoring, staff training, data protection and online classroom arrangements.

15. Related policies and guidance

This policy should be read alongside Tecnis Academy's Child Protection/Safeguarding Policy, Privacy/Data Protection Policy, Staff Code of Conduct, Acceptable Use Policy, Complaints Policy and relevant behaviour and disciplinary procedures.

Tecnis will keep this policy under review against relevant current guidance, including the Department for Education's Keeping Children Safe in Education 2026, safeguarding and remote education guidance, filtering and monitoring standards, data-protection guidance, Working Together to Safeguard Children, and relevant Information Commissioner's Office guidance on children's data and online services.

This policy is informed by the safeguarding principles and relevant requirements in these sources insofar as they apply to Tecnis Academy and its educational arrangements.