# Thames Hightech Ltd
# Online Safety Policy 2025/26

*Registered address: Hurlingham Studio, Ranelagh Gardens, London SW6 3PA*
*DSL / Online Safety Lead: Yuhong Li | Contact: Andrew.li@thameshightech.com | 07538826068*

Thames Hightech Ltd recognises that online safety is an essential part of safeguarding and promoting the welfare of children and young people. Students may be exposed to significant risks through phones, tablets, laptops, gaming platforms, social media, messaging apps, email, online learning platforms and other digital services.

This policy explains how Thames Hightech Ltd seeks to reduce online risk, support safe use of technology, respond to incidents and work with students, homestays, parents and schools to promote safe and responsible behaviour online.

This policy should be read alongside the Safeguarding and Child Protection Policy, Staff and Homestay Code of Conduct, Anti-Bullying Policy, Anti-Radicalisation / Prevent Policy, Missing Student Procedure, Data Protection Policy, Student Handbook and Homestay Handbook.

## 1. Key principles

- Online safety is a safeguarding matter.
- The welfare of the child is paramount.
- Students should be educated and supported to use technology safely rather than simply restricted without explanation.
- Online abuse can happen between peers, from adults to children, or as part of wider abuse, exploitation or coercion.
- Concerns must be reported and addressed promptly.

## 2. Scope

This policy applies to Thames Hightech Ltd staff, contracted staff, volunteers, local coordinators, homestays and students whenever students are under the care, supervision or support of Thames Hightech Ltd, including during homestay stays, transport arrangements, welfare support and online communication.

## 3. Roles and responsibilities

The Director / DSL has lead responsibility for online safety. Staff and homestays are expected to remain alert to online risks, model appropriate online behaviour, report concerns and support students to stay safe. Students are expected to use devices and the internet responsibly and to seek help if something worries them. Parents and schools may also play a role in information sharing and support.

- Yuhong Li is the DSL and online safety lead.
- All staff and homestays must report online safety concerns in line with safeguarding procedures.
- Homestays are expected to maintain a reasonably safe digital environment and supervise use in an age-appropriate way.

## 4. Categories of online risk

Online safety risks can be grouped under four broad headings:

- Content: exposure to harmful, illegal or inappropriate material such as pornography, self-harm content, hateful material, extremist content, or misleading information.
- Contact: harmful interaction with others online, including grooming, coercion, exploitation, radicalisation, bullying, pressure or fraud.

- Conduct: unsafe or harmful online behaviour by the user, including sharing personal information, sending or receiving explicit content, cyberbullying, harassment or misuse of devices.
- Commerce: online scams, phishing, financial exploitation, gambling, inappropriate advertising and other financially harmful activity.

## 5. Examples of online safeguarding concerns

- Cyberbullying, harassment or online humiliation.
- Grooming or inappropriate online contact from adults or older peers.
- Sharing of nudes or semi-nude images, coercion to send images, or threats involving images.
- Exposure to harmful sexual content or pornography.
- Online radicalisation or extremist influence.
- Online fraud, phishing or financial exploitation.
- Exploitation through gaming, social media or messaging platforms.
- Persistent secrecy, distress or behavioural change linked to online activity.

## 6. Expectations for staff and homestays

- Adults must communicate with students professionally and appropriately.
- Adults must not use personal social media relationships with students or secretive messaging channels.
- Adults should be familiar with this policy and relevant safeguarding guidance.
- Homestays should take reasonable steps to supervise and support safe use of devices and the internet according to the student's age and circumstances.
- Adults must not search devices, view images or delete material except where there is a clear reason and in accordance with safeguarding procedures.

## 7. Expectations for students

- Students should protect personal information, passwords and location data.
- Students should not share explicit images, engage in bullying or use technology to intimidate or harm others.
- Students should speak to a trusted adult if something online makes them feel uncomfortable, unsafe, pressured or frightened.
- Students should follow school rules, Thames Hightech Ltd guidance and any reasonable homestay expectations about devices, Wi-Fi and bedtime routines.

## 8. Homestay digital environment

Homestays are expected to take reasonable and proportionate steps to help provide a safe online environment. Depending on the age and needs of the student, this may include:

- Using parental controls, filters or router settings where appropriate.
- Setting expectations about suitable screen use, privacy, device charging and overnight use.
- Discussing safe use of social media, gaming and messaging apps.
- Encouraging students to report anything upsetting or inappropriate.

Thames Hightech Ltd recognises that homestays are private homes and not schools. The expectation is therefore one of reasonable safeguarding support rather than school-style technical monitoring systems.

## 9. Recognising warning signs

Possible indicators of online harm may include:

- A marked increase or decrease in time spent online.
- Becoming secretive, withdrawn, distressed or angry after device use.
- New contacts, hidden accounts or unexplained communication patterns.
- Pressure to keep conversations secret.
- Evidence of bullying, blackmail, threats or sexualised online behaviour.
- Sudden requests for money, secrecy about purchases, or signs of fraud.

## 10. Responding to concerns

Any online safety concern should be treated as a potential safeguarding concern and responded to promptly.

- Listen, reassure and record. Do not promise absolute confidentiality.
- Report the concern to the DSL as soon as possible.
- Do not investigate alone or ask leading questions.
- Do not forward, share or circulate concerning material.
- Do not search devices or view images unless there is a clear and justifiable reason and the appropriate safeguarding procedure is followed.

## 11. Viewing images and device handling

Where a concern involves nudes, semi-nudes or other explicit material, Thames Hightech Ltd will follow current safeguarding guidance and act proportionately.

- Images should not be viewed unless there is a clear reason to do so and no alternative is available.
- If viewing is necessary, it should be done by the DSL or another appropriate senior person, with another adult present where possible.
- Any decision to view, seize or request deletion of material must be recorded with reasons.
- Where the matter indicates exploitation, coercion, abuse or immediate risk, the police and/or children's services must be contacted.

## 12. Referral to other agencies

The DSL will consider whether the concern should be referred to police, children's services, the school DSL, CEOP or another relevant agency.

- Call 999 where there is immediate danger.
- Use 101 for non-emergency police reports where appropriate.
- CEOP may be relevant for sexual abuse or grooming online.
- Schools should be informed where the issue affects the student's welfare, behaviour or peer relationships.

## 13. Support for students

Students affected by online incidents may need reassurance, practical help and emotional support. Thames Hightech Ltd will consider what support is needed, which may include communication with parents, school-based support, safeguarding planning or signposting to specialist services.

## 14. Education and awareness

Thames Hightech Ltd supports online safety through its policies, handbooks, conversations with students, communication with homestays and safeguarding culture. Staff and homestays should be familiar with current online risks, including grooming, bullying, image sharing, fraud, radicalisation and harmful content.

## 15. Useful reporting and support routes

- DSL: Yuhong Li – 07538826068 – Andrew.li@thameshightech.com
- Emergency services: 999
- Police non-emergency: 101
- Childline: 0800 1111
- CEOP reporting: www.ceop.police.uk/safety-centre
- Thinkuknow: www.thinkuknow.co.uk
- NSPCC online safety resources: www.nspcc.org.uk

## 16. Review

This policy will be reviewed at least annually and sooner if guidance, legislation, AEGIS standards or organisational practice changes.

| | |
|---|---|
| Version | 2025/26 |
| Approved by | Yuhong Li, Director / DSL |
| Effective date | 1 September 2025 |
| Review date | 1 September 2026 |
| Contact | Andrew.li@thameshightech.com \| 07538826068 |