THAMES
HIGHTECH LIMITED

Hurlingham Studio, Ranelagh Gardens

London

SW6 3PA

Thames Hightech Ltd Online Safety Policy

Policy Statement

This document is based on the most recent guidance from the Department for Education Keeping Children Safe in Education, and NSPCC advice on Online Safety. The effectiveness of the policy will be monitored and reviewed annually through the number of reported incidents of a breach of online safety.

Staff and Homestays

The Thames Hightech Ltd Code of Conduct for Staff and homestays has been made available and explained to staff and homestays to ensure that there is an awareness of how to communicate online with students as well as how to minimise the risks attached to digital and video images of them. Homestays play a crucial role in ensuring that the students who stay with them use the internet and mobile devices in accordance with the guidance contained within this policy and the Homestay Handbook. The DSL takes the lead with online safety and will deal with any concerns raised as outlined in the procedures included in this policy.

Training

Thames Hightech Ltd's DSL will complete additional online safety training where this is not sufficiently covered within their safeguarding training undertaken and will then ensure that the appropriate information is disseminated to all staff and homestays.

Key Safeguarding Contact Details

Role	Name	Telephone	Email
Designated Safeguarding Lead	Yuhong Li	07538826068	Andrew.li@thameshightech.com

Students

Students are responsible for using the internet and mobile devices in accordance with the guidance in the Student Handbook. Students will be informed about the importance of adopting good online safety practice and reporting misuse, abuse or access to inappropriate materials and how to report these concerns. Thames Hightech Ltd further supports students in raising their awareness of how to stay safe online through our social media updates, policies and website.

Online Safety – Areas of risk

It is essential that students are safeguarded from potentially harmful and inappropriate online material. An effective approach to online safety empowers a school, college, guardian or homestay to protect and educate children in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

What is online abuse?

The NSPCC define online abuse as any type of abuse that happens on the internet. It can happen across any device that's connected to the web, like computers, tablets and mobile phones. And it can happen anywhere online, including:

- social media,
- text messages and messaging apps,
- emails,

- online chats,
- playing online games
- live streaming sites.

Children and young people may experience cyberbullying (bullying that takes place using technology including social media sites, mobile phones, gaming sites), grooming (building an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking), sexual abuse, 'sexting' or youth produced imagery, sexual exploitation, county lines gang recruitment, radicalisation or emotional abuse from people they know as well as from strangers. It might be part of other abuse which is taking place offline, like bullying or grooming. Or the abuse might only happen online.

Thames Hightech Ltd clearly has a role to play in reporting signs of possible online abuse early so that prompt action can be taken to protect any children who are found to be at risk. Thames Hightech Ltd has a policy for Anti-bullying (including cyber-bullying) that outlines how incidences of cyber-bullying will be addressed.

Possible signs of online abuse:

The NSPCC list possible signs of a child experiencing abuse online if they demonstrate a change in behaviour or unusual behaviour:

• spend a lot more or a lot less time than usual online, texting, gaming or using social media
• seem distant, upset or angry after using the internet or texting
• be secretive about who they're talking to and what they're doing online or on their mobile phone
• have lots of new phone numbers, texts or email addresses on their mobile phone, laptop or tablet.

Some of the signs of online abuse are similar to other abuse types, including cyberbullying, grooming, sexual abuse, child sexual exploitation. These can be found on the NSPCC website https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/

The possible signs of abuse could be seen through reports from students or schools, incident reporting by staff, and/or Local Co-ordinator reports. In response to a safeguarding report the matter would be dealt with in accordance with the 'Safeguarding and Child Protection' Policy and Process.

Set Boundaries

Thames Hightech Ltd encourage staff and homestays to set an appropriate agreement with students in order to supervise internet access and set boundaries about what they can and cannot do online. If a child breaks the rules, we would ask the homestay to restrict internet access for an agreed period of time.
Below is some suggested advice for talking to children about online safety:
https://www.thinkuknow.co.uk/parents/articles/having-a-conversation-with-your-child/
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/talking-your-child-staying-safe-online/

Filters and monitoring

Thames Hightech Ltd asks homestays to be doing all that they reasonably can to limit children's exposure to the above risks from the IT systems at the home. As part of this process, homestays should ensure appropriate filters and monitoring systems are in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, homestays should consider the age range of their pupils, the number of pupils, and how often they access the IT system.

Homestays are asked to use privacy settings, parental controls and built-in internet safety features provided by the major internet service providers. The UK Safer Internet Centre has guides for parental controls (homestays) https://saferinternet.org.uk/online-issue/parental-controls https://saferinternet.org.uk/online-issue/parental-controls

The NSPCC provide advice for homestays on parental controls which allow a number of different things to happen including planning what time of day children can go online for, filtering and blocking content, setting different profiles so that each family member can access age appropriate content and restricting information that can be shared: https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/

Staying safe on mobiles, smartphones and tablets

The NSPCC has advice for staying safe on all types of devices, including mobiles, smartphones and tablets. Full details can be found on the website:
https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Childline also provide useful information for students:

https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/
This includes guidance on a range of issues, including specific guidance on mobile phones safety and sexting.

Information on sexting and sending nudes can be found here:

https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/sexting-sending-nudes/

Childnet have produced a very useful guidance for students who have made a mistake sending nude pictures:

https://www.childnet.com/help-and-advice/nudes-11-18-year-olds/

Social network sites

Children and young people connect online with friends, make new friends and browse the internet for information, chat with others and play games. This may include using search engines, sharing images, watching videos, using social network sites, playing games and chatting with people through online gaming.

Homestays are advised to ensure that their own children and/or Thames Hightech Ltd students know where the reporting functions are on each of the sites they use, how to block someone and how to keep information private.

The NSPCC encourage talking to children about apps, games and social media using 'Net Aware' to stay up to date on the latest social networks, apps and games children are using and what you need to know about for example reporting and privacy settings:
https://www.net-aware.org.uk/

The NSPCC encourage talking to children about online safety:
https://www.nspcc.org.uk/keeping-children-safe/online-safety/talking-child-online-safety/

Further reading:
NSPCC Online Safety: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Child Exploitation and Online Protection Centre:
CEOP: Child Exploitation & Online Protection Centre – internet safety
CEOP: Thinkuknow: https://www.thinkuknow.co.uk/

UK Safer Internet Centre:
https://www.saferinternet.org.uk/

Disrespect Nobody – find out about healthy relationships and respecting each other:
https://www.disrespectnobody.co.uk/

Internet matters – helping parents keep their children safe online:
https://www.internetmatters.org/

How social media is used to encourage travel to Syria and Iraq: A briefing note
https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Procedure for dealing with an incident which involves online services:

1. Thames Hightech Ltd staff member receives the report of suspected breach in online safety from a student, parent or other source by face-to-face disclosure, email or telephone call.
2. Thames Hightech Ltd Staff member adheres to the Safeguarding and Child Protection Policy including contemporaneously recording the disclosure in the most appropriate format (using the 'Tell Explain Describe' model if the information is being given by a student).
3. The record of the disclosure is reported verbally as soon as practicable to the Designated Safeguarding Lead (DSL). The staff member must submit a written record of the disclosure to the DSL.
5. The DSL will hold an emergency strategy meeting to discuss the incident, assess the alleged threat and risk to the child (including any relevant facts about the child which may affect their vulnerability including age and ability), implement an action plan and continue to review the situation until a resolution has been achieved.
6. The meeting will be recorded with timed and dated entries within an incident record to record all actions and updates.
7. The DSL will arrange for the young person to be helped and supported in recognition of the pressures (and possible vulnerabilities) they may have been under as a result of the suspected abuse. This could include helping them to understand how to recognise the early signs of online abuse, the wider issues and motivations of online abuse and making available relevant information and material. This help and support could be provided from accredited organisations such as the school, National Society for the Prevention of Cruelty to Children (NSPCC), Childline, National Crime Agency (NCA), Child Exploitation and Online Protection Centre

(CEOP) websites and helplines.

8. The DSL will ensure that viewing of any images or other content is only made where there are good and clear reasons to do so (unless unavoidable because the student has willingly shown a member of staff), basing incident decisions on what the DSL has been told about the content of any imagery or other content.

The DSL will ensure that staff members do not search through devices and delete imagery unless there is a good and clear reason to do so. If the DSL feels that it is necessary to view any imagery, they will follow the guidance in the guidance Sharing nudes and semi-nudes: advice for education settings working with children and young people (publishing.service.gov.uk). This includes ensuring that there is another senior member of staff present, ideally of the same sex of the as the student in the images when the viewing takes place. (The publication Sharing nudes and semi-nudes: advice for education settings working with children and young people explains the procedure to follow if it is felt that there is a clear reason to view such imagery in section 2.10.)

9. The DSL will consider the need to ask for the student to produce the device as evidence. The viewing of any images, other content or seizing of any devices will be recorded including those present, date and time.

10. The DSL will consider the need to contact another school, college, setting or individual and whether to contact the parents or carers of the children involved. In most cases parents should be involved unless there is good reason to believe that involving these parties would put the young person at risk of harm.

11. The incident will be referred to a statutory agency (Children's Services on the Local Authority telephone number or the police by dialling 101) immediately if there is a concern a young person has been harmed or is at immediate risk of harm (telephone the police by dialling 999). This would include information coming to light if at the initial stage:

• The incident involves an adult

• There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)

• What you know about any imagery or other content suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent

• Any imagery or other content involves sexual acts and any pupil in the imagery is under 13

• You have reason to believe a pupil or pupil is at immediate risk of harm owing to

the sharing of any imagery, for example, the young person is presenting as suicidal or self-harming. Where the material or activities found or suspected are illegal and there is no immediate risk to the child, The Child and Exploitation Online Paedophile Unit should be informed. If none of the above apply, the DSL may decide (with input from key stakeholders if appropriate) to respond to the incident without involving the police or children's social care. The DSL can choose to escalate the incident at any time if further information/concerns come to light. The decision should be recorded in line with the Safeguarding Policy and Child Protection Policy, and regularly reviewed throughout the process of responding to the incident.

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved, and the risks can be managed within Thames Hightech Ltd support framework and network for the child.

12. If the DSL has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery or other content to limit any further sharing. In most cases, children and young people should be asked to delete the imagery or content and to confirm that they have deleted them. They should be given a deadline for deletion across all devices, online storage or social media sites. They should be reminded that possession of nudes and semi-nudes is illegal (if this is what the issue was). They should be informed that if they refuse or it is later discovered they did not delete such imagery, they are continuing to commit a criminal offence and the police may become involved. A record will be made of these decisions as per the Safeguarding Policy including decisions, times, dates and reasons.

Any decision to search a child or young person's device and delete imagery will be based on the professional judgement of the DSL (or equivalent) and will always comply with the safeguarding and child protection policy and procedures of Thames Hightech Ltd. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers will also be informed unless this presents a further risk to any child or the young person.

13. Where the DSL is aware that youth produced sexual imagery or other content has been unavoidably viewed by a member of staff, the DSL should ensure that the staff member has appropriate support. Viewing youth produced sexual imagery or other content can be distressing for both young people and adults and appropriate emotional support may be required.

14. Where police action has been instigated for an incident involving a member of

staff, homestay or volunteer, Thames Hightech Ltd internal procedures will take place at the conclusion of the police action. A suspension will be likely to take place before the internal procedures begin.

Responding to an incident of the sharing of nudes and semi-nude imagery

As mentioned above, Thames Hightech Ltd will follow the guidance in Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk) when responding to an incident of sharing nudes and semi-nudes.

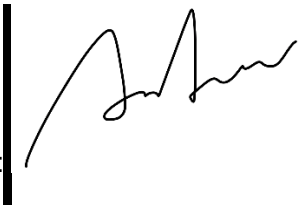
Remote learning

Staff and homestays should be aware that where students are being asked to learn online at home, schools will have a remote learning policy which should be referred to when homestays and guardians are supporting a student to learn remotely. The DfE has provided advice to support schools and colleges do so safely, including Safeguarding and remote education - GOV.UK (www.gov.uk)The NSPCC also provide helpful advice: Undertaking remote teaching safely | NSPCC Learning

Review

We are committed to reviewing our policy and good practice annually.

This policy was last reviewed on: 19/04/2024

Signed: 

Date: 19/04/2024