POLICY · 2026–27

Online Safety Policy

Policy Statement

This document is based on the most recent guidance from the Department for Education, Keeping Children Safe in Education 2026, and NSPCC advice on Online Safety. WBS Guardians carries out an annual review of its approach to online safety, supported by an annual online safety risk assessment that considers and reflects the risks our students face (see 'Annual review and online safety risk assessment' below). The review also considers any reported incidents and changes in UK safeguarding guidance and legislation on children's use of social media and online safety.

Staff and Homestays

The WBS Guardians 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

The WBS Guardians DSL and DDSL 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.

Annual review and online safety risk assessment

Technology, and the risks and harms related to it, evolve and change rapidly. Each September, as part of the annual policy review, the DSL (with the DDSL) completes the WBS Guardians Online Safety Risk Assessment. This considers the risks our students currently face (including content, contact, conduct and commerce risks, AI-generated imagery and chatbots, sextortion, online radicalisation, gaming and gambling), the controls in place in homestays and in our own communications, and any incidents, concerns or new guidance from the previous year. Actions arising are recorded, assigned and reviewed termly.

The policy is also reviewed whenever there is a significant change in guidance or legislation, including Keeping Children Safe in Education, the Online Safety Act 2023 and Ofcom's codes of practice for protecting children online, and any new government rules on children's use of social media. Key changes are shared with staff and homestays in the annual safeguarding update.

Key Safeguarding Contact Details

ROLE	NAME	TELEPHONE NUMBER	EMAIL
Designated Safeguarding Lead (DSL)	Iain Howell	07984 925526	iain@whichbritishschool.com

ROLE	NAME	TELEPHONE NUMBER	EMAIL
Deputy Designated Safeguarding Lead (DDSL)	Jennifer Britton (Co-founder and Director)	07540 868974	jennifer@whichbritishschool.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. WBS Guardians 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 students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).
- Artificial intelligence (AI): Keeping Children Safe in Education 2026 highlights emerging risks from AI, including images and videos that have been digitally altered or wholly generated using AI (sometimes described as ‘deepfakes’ or ‘deep nudes’), AI chatbots and image-manipulation (‘nudify’) apps. Creating or sharing an AI-generated or altered nude or semi-nude image of a child is treated in exactly the same way as sharing a real image and must be reported to the DSL or DDSL.

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.

WBS Guardians 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. WBS Guardians 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 or homestays. 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

WBS Guardians 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:

Having a conversation with your child (thinkuknow.co.uk)
Teaching Your Child about Internet & Online Safety | NSPCC

Filters and monitoring

WBS Guardians 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

WBS Guardians will make every homestay aware of the wi-fi controls and filtering options available to them at their annual visit, and will check, at least once a year, that appropriate filtering and parental controls are in place on the home network and devices available to students. The outcome is recorded on the annual homestay checklist.

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, using apps, playing games and chatting with people through online gaming.

Homestays are advised to ensure that their own children and/or WBS Guardians 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 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: CEOP Education (thinkuknow.co.uk)

UK Safer Internet Centre:
Homepage - UK Safer Internet Centre

Internet matters – helping parents keep their children safe online:
Information, Advice and Support to Keep Children Safe Online (internetmatters.org)

The use of social media for online radicalisation - GOV.UK (www.gov.uk)

Procedure for dealing with an incident which involves online services:

1. A WBS Guardians staff member receives a report of a suspected breach of online safety from a student, parent or other source, by face-to-face disclosure, email or telephone call.

2. The staff member follows the Safeguarding and Child Protection Policy, including recording the disclosure contemporaneously in the most appropriate format (using the 'Tell, Explain, Describe' model if the information is given by a student).

3. The disclosure is reported verbally as soon as practicable to the Designated Safeguarding Lead (DSL), or in their absence the Deputy DSL (DDSL), and the staff member submits a written record of the disclosure to the DSL (or DDSL).

4. The DSL holds 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, such as age and ability), implement an action plan and keep the situation under review until it is resolved.

5. The meeting is recorded with timed and dated entries in an incident record of all actions and updates.

6. The DSL arranges 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 recognise the early signs of online abuse and the wider issues and motivations behind it, and making relevant information available. Support can also come from accredited organisations such as the school, the NSPCC, Childline, the National Crime Agency (NCA) and the Child Exploitation and Online Protection command (CEOP).

7. The DSL will ensure that images or other content are only viewed where there are good and clear reasons to do so (unless this is unavoidable because the student has willingly shown a member of staff), basing decisions on what the DSL has been told about the content. Staff must not search through devices or delete imagery unless there is a good and clear reason to do so. If the DSL feels it is necessary to view any imagery, they will follow 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' (section 2.10), including ensuring that another senior member of staff is present, ideally of the same sex as the student in the images.

8. The DSL will consider whether to ask the student to produce the device as evidence. The viewing of any images or other content, and the seizing of any device, will be recorded, including who was present and the date and time.

9. The DSL will consider whether 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 this would put the young person at risk of harm.

10. The incident will be referred immediately to a statutory agency (children's social care for the area where the child lives or is staying, or the police on 101; or 999 if a young person is at immediate risk of harm) if at the initial stage:

- the incident involves an adult;
- there is reason to believe that a young person has been coerced, blackmailed (including financially motivated sexual extortion, 'sextortion') or groomed, or there are concerns about their capacity to consent (for example owing to special educational needs);
- what is known about the imagery or other content suggests it 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 child in the imagery is under 13; or
- there is reason to believe a student 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 activity found or suspected is illegal and there is no immediate risk to the child, the Child Exploitation and Online Protection command (CEOP) of the National Crime Agency will be informed.

11. If none of the above apply, the DSL may decide (with input from key stakeholders where appropriate) to respond to the incident without involving the police or children's social care. This decision will only be made where the DSL is confident they have enough information to assess the risks to the children involved and that the risks can be managed within WBS Guardians' support framework and network for the child. The DSL can escalate the incident at any time if further information or concerns come to light. The decision will be recorded in line with the Safeguarding and Child Protection Policy and reviewed throughout.

12. If the DSL has decided that other agencies do not need to be involved, consideration will be given to deleting imagery or other content to limit further sharing. In most cases, children and young people will be asked to delete the imagery or content and confirm that they have done so, within a set deadline, across all devices, online storage and social media. They will be reminded that possessing nudes and semi-nudes of under-18s is illegal, and that if they refuse, or it is later discovered that they did not delete the imagery, they are continuing to commit a criminal offence and the police may become involved. Decisions, times, dates and reasons will be recorded.

13. 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 DDSL) and will always comply with the Safeguarding and Child Protection Policy. All decisions will be recorded, including times, dates and reasons, and logged in the safeguarding records. Parents and carers will be informed unless this presents a further risk to any child.

14. Where the DSL is aware that nude or semi-nude imagery or other content has been unavoidably viewed by a member of staff or homestay, the DSL will ensure that they receive appropriate support, as viewing such content can be distressing.

15. Where police action has been instigated for an incident involving a member of staff, homestay or volunteer, WBS Guardians' internal procedures will take place at the conclusion of the police action. A suspension is 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, WBS Guardians 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: 28/09/2026. Next review: September 2027.

Amended: 29/10/2026 (annual review and online safety risk assessment, legislation review, annual filtering check, procedure renumbered).

Signed: Iain Howell, CEO and DSL

Date: 28/09/2026

WBS Guardians · Which British School
71–75 Shelton Street, Covent Garden, London WC2H 9JQ · 24 hours: 07984 925526 / 07540 868974 · guardians@whichbritishschool.com
WBS Guardians is a trading name of Which Independent Schools Ltd., registered in England and Wales, company no. 09287591.

AEGIS ACCREDITED