Online Safety Policy

APRIL WELL LIMITED — Company No. 11924473

Registered office: Unit 39c St Olavs Court Business Center, Lower Road, London, England, SE16 2XB

Director / Legal Representative: Xiaoying Chi

Designated Safeguarding Lead (DSL): Xiaoying Chi

(Deputy DSL: n/a – temporarily covered by the DSL)

24/7 emergency: 07930416543

Email: info@aprilwell.co.uk

This policy is publicly available. It may be shared with parents, agents, partner schools and inspectors on request. A copy is provided to staff and relevant accommodation adults and made available to students and parents on request.

Document Control

Title: Online Safety Policy

Owner: Xiaoying Chi, Director / DSL

Approved by: Xiaoying Chi

Document ID: AWP-OSP-02

Version: v2.0 (21 October 2026)

Issue date: 21 October 2026

Next review: 21 October 2027 *(or earlier if law/policy changes)*

Status: Public

Distribution: Company website; Student/Parent Handbooks; provided to schools and inspectors on request.

This document is reviewed annually in October and whenever statutory guidance or AEGIS Standards change.

Table of Contents

Training **1**

Key Safeguarding Contact Details **1**

What is online abuse? **2**

Possible signs of online abuse: **3**

Staying safe on mobiles, smartphones and tablets **4**

Social network sites **5**

Procedure for dealing with an incident which involves online services: **6**

Responding to an incident of the sharing of nudes and semi-nude imagery ***9***

Remote learning ***9***

The Prevent Duty ***9***

Review ***9***

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. The effectiveness of the policy will be monitored and reviewed annually through the number of reported incidents of a breach of online safety.

April Well Limited is a small guardianship organisation. Students supported by April Well normally live in boarding accommodation at their schools or with their parents. April Well Limited does not provide routine or long-term homestay accommodation. However, April Well may arrange or coordinate short-term emergency accommodation in clearly defined emergency or exceptional situations, in accordance with its Emergency Procedure and safeguarding policies. References in this policy to "homestays" include any host family, emergency accommodation adult or accommodation arrangement used or approved by April Well Limited.

Staff and Homestays

The April Well Limited Code of Conduct for Staff and Homestays has been made available and explained to staff and, where applicable, to any homestays, emergency accommodation adults or other accommodation arrangements used or approved by April Well Limited. This ensures that relevant adults are aware of how to communicate online with students and how to minimise the risks attached to digital and video images of them. Where April Well Limited uses or approves homestays, emergency accommodation adults or other accommodation arrangements, the responsible adults must ensure that students use the internet and mobile devices in accordance with the guidance contained within this policy and any relevant accommodation guidance.

The Designated Safeguarding Lead (DSL) takes the lead with online safety and will deal with any concerns raised as outlined in the procedures included in this policy.

Training

April Well Limited's DSL will complete additional online safety training where this is not sufficiently covered within their safeguarding training and will then ensure that the appropriate information is disseminated to all staff and, where applicable, to any homestays, emergency accommodation adults or other accommodation arrangements used or approved by April Well Limited.

Key Safeguarding Contact Details

Role	Name	Telephone Number	Email
Designated Safeguarding Lead (DSL)	Xiaoying Chi	+44 (0)7930 416543	info@aprilwell.co.uk

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. April Well Limited 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, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- 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 (including AI-generated or digitally altered imagery), consensual and non-consensual sharing of nudes and semi-nudes, pornography 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.

April Well Limited 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. April Well Limited 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

April Well Limited encourages staff, parents and, where applicable, any homestays, emergency accommodation adults or other accommodation arrangements used or approved by April Well Limited to set appropriate boundaries with students about internet access and what they can and cannot do online. If a student breaches agreed online safety rules, April Well Limited would ask the responsible adult, for example a parent, house parent or approved accommodation adult, to take appropriate safeguarding action, which may include restricting 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

Where April Well Limited uses or approves homestays, emergency accommodation adults or other accommodation arrangements, April Well expects the responsible adults to do all that they reasonably can to limit students' exposure to the above risks from IT systems in the accommodation. As part of this process, responsible adults should ensure that appropriate filters, monitoring arrangements, privacy settings and parental controls are considered, taking into account the age of the students, the number of students, and how often they access the IT system.

Responsible adults are asked to use privacy settings, parental controls and built-in internet safety features provided by the major internet service providers. April Well will make relevant adults aware of available wi-fi controls and filtering options. Mobile data can bypass wi-fi filtering. The UK Safer Internet Centre has guides for parental controls (homestays)
https://saferinternet.org.uk/online-issue/parental-controls

The NSPCC provide advice 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.

Where April Well Limited uses or approves homestays, emergency accommodation adults or other accommodation arrangements, responsible adults are advised to ensure that students know where the reporting functions are on each of the sites they use, how to block someone and how to keep information private. Follow current service age restrictions and law. The DSL will monitor announced social media changes planned for spring 2027 and update advice when regulations and commencement are confirmed; an under-16 ban is not yet in force.

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)

How social media is used to encourage travel to Syria and Iraq: A briefing note

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

Procedure for dealing with an incident which involves online services:

1. April Well Limited 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. April Well Limited 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 immediately to the Designated Safeguarding Lead (DSL). The staff member must submit the initial written record promptly and no later than 24 hours after becoming aware; do not delay protection or external referrals. In immediate danger call 999 without waiting for internal approval. If the DSL is unavailable, use vetted cover under the Emergency Procedure; do not delay external referrals. If the concern involves the DSL, report directly to the relevant local authority LADO and police or children's social care as appropriate.
4. The DSL will promptly assess immediate safety and arrange an internal review 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. Internal meetings must not delay police or children's social care referrals or interfere with their enquiries.
5. The meeting will be recorded with timed and dated entries within an incident record listing all actions and updates.
6. 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.

7. 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. Frontline staff must not view, copy, save, forward or delete suspected child sexual imagery, or ask a child to send it. Accidental viewing must be reported immediately. 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 - GOV.UK (www.gov.uk). Exceptional viewing must follow section 2.10 safeguards; another staff member should be present but need not view the image. Wherever possible the viewer should be of the same sex as the child. (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.)

8. The DSL will seek police advice about preserving the device as evidence; staff must not compel access or seize it under powers reserved to schools or police. The viewing of any images, other content or seizing of any devices will be recorded including those present, date and time.

9. 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.

10. 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 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. Suspected online child sexual abuse or grooming may also be reported to NCA-CEOP. Other suspected offences go to police; CEOP is not an emergency service or a substitute for required referrals. 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 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 April Well Limited support framework and network for the child.

11. Any deletion must follow section 2.10 of the UKCIS guidance, with police advice where needed; preserve possible evidence and never delete while a referral or investigation requires it. If other agencies do not need to be involved, consider deletion to prevent 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. Explain the law on indecent images of under-18s and possible police involvement without blaming or shaming the child; not every nude image is legally indecent. A record will be made of these decisions as per the Safeguarding and Child Protection Policy, including decisions, times, dates and reasons.

April Well does not acquire schools' statutory search or confiscation powers by following this guidance. Any access to a student's device requires a lawful basis and must comply with the Safeguarding and Child Protection Policy and procedures of April Well Limited. 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.

April Well Limited may also invoke measures under the Student Behaviour Code of Conduct to discourage young people from sharing, creating or receiving inappropriate images.

12. 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.

13. Where police action has been instigated for an incident involving a member of staff, homestay or volunteer, April Well Limited will agree the timing of internal enquiries with police and the LADO. Immediate safeguarding action and necessary referrals must not wait for police action to conclude. Suspension is not automatic: assess risk, consider alternatives and record reasons with appropriate LADO/police advice.

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

As mentioned above, April Well Limited 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. These risks also include AI-generated sexual imagery, harmful interactions with AI chatbots and financially motivated sexual extortion. Report concerns through the same safeguarding procedure. Apply the staff allegations/low level concerns procedures and AEGIS self-reporting requirements where relevant; do not delay statutory referrals.

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 parents, homestays or 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: Safeguarding and child protection for tutors

The Prevent Duty

April Well Limited pays due regard to the Prevent Duty and recognises that there is a risk of students being exposed to radicalisation or extremist views online. Signs of online radicalisation may include spending increasing amounts of time talking to people with extreme views online, or searching inappropriate websites linked to terrorism ideology. Staff and homestays should remain vigilant and report any concerns to the DSL. Please see our anti-radicalisation policy for further details.

Review

The DSL will review online safety annually with a documented assessment of students' risks and controls (AEGIS 6.10.2), and sooner when risks, UK guidance or legislation change.

This policy was last reviewed on: 21/10/2026

Signed: 

Name: Xiaoying Chi

Role: Director and Designated Safeguarding Lead (DSL)

Date: *21/10/2026*