Online Safety Policy

Created by:	Jonathan Horleston-Wilkes
Approved by:	All trustees at online teams meeting, recorded in minutes
Approval date:	13/01/2026
Next review date:	January 2028

Online Safety Definition

Eagle's Nest Project takes the safety and welfare of all those with whom it is connected very seriously. We recognise that technology and the internet can be a fantastic tool for young people, allowing them to talk to friends, be creative and have fun. However, just like in the real world, sometimes things can go wrong and the use of technology has become a significant component of many safeguarding issues. We believe that children and young people should never experience abuse of any kind and, as such, recognise that safeguards need to be in place to support the safe use of electronic devices and internet access to ensure that all young people and adults involved in our organisation are protected from potential harm online.

e-Safety – or electronic safety is the collective term for safeguarding involving the use of mobile phones, computers (laptops, netbooks, tablets) and other electronic devices including games consoles, to communicate and access the Internet, emails, texts messages (SMS), Direct Messaging (DM), social networking sites (SNS) and other social media as well as the use of AI (Artificial Intelligence); often referred to as Information and Communications Technology (ICT).

The technology is constantly advancing bringing with it additional safeguarding considerations, but the risks can be categorised into four areas:

- Content- exposure to harmful content
- Contact- subject to harmful online interaction
- Conduct- own online conduct that increases likelihood of, or causes, harm
- Commerce- financially linked risk on online (e.g. gambling, inappropriate advertising, scams)

An online safety policy should be adopted and adapted to reflect all communications between Eagle's Nest employees (staff team and volunteers) and the young people we work with, recognising the merging between online and offline worlds and the need to define clear boundaries for everyone.

This policy seeks to outline the procedures in place to limit exposure to safeguarding issues through ICT, helping to both protect and educate those we work with. We aim to support them to develop skills to identifying and avoid risk, learning how best to protect themselves and their friends, and knowing how to get support and report abuse if they do encounter difficulties. As an organisation, we appreciate the value of technology and seek to find a balance that both safeguards staff and students, whilst not limiting the valuable learning resource that the internet provides.

Safety and Support Measures

We will seek to keep young people and employees safe through filtering and monitoring:

- By asking all students to hand in mobile devices when attending sessions in order to both prevent distraction and limit access to internet and online games and apps whilst in sessions, including messaging friends and family. The Wifi password at the centre will not be shared with any students. These measures avoid unsupervised use of internet and social media and reduce the risk of upset and anxiety caused by friends and family messaging during education time.

- By limiting internet access in sessions to fully supervised, so that this is only available on laptops/PCs or I-Pads when there is a member of staff present and is therefore being used for linked educational activities. Whilst we currently do not have networked computers, and therefore a formal filtering system, all devices have firewall settings and passwords and are used under direct supervision of staff. Whilst it may be that in certain circumstances to build relationship, staff allow students to share their favourite music track from YouTube or other similar sites, this should not be encouraged in general, and if used as a bridge building activity, staff must maintain control and stop the music and lock the device should either the video or lyrics be inappropriate.

- By physically monitoring all computer use by students, whether on- or offline, during sessions. Any work that is being created by the students will be fully reviewed by staff before anything is taken away from the session (via hard copy or electronically). If a student refuses to allow this full review, then the use of the computer must be stopped, and nothing may be taken away from the session.

- By seeking educational opportunities with young people to discuss the appropriate use of the internet and social media, including formal sessions using CEOP/ Youthscape and other relevant resources to help them identify potential risks.

- By supporting and encouraging parents and carers to do what they can to keep their children safe online, including highlighting any concerns that arise through conversations with young people and signposting to websites and resources that can provide them with further support.

- By providing clear and specific directions to staff and volunteers on how to behave online through our staff Code of Conduct, which includes specific guidance on the various forms of communication and how to manage these effectively.

- By providing supervision, support and training for staff and volunteers about online safety and dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, Change, sexual abuse and sexual exploitation.

- By issuing guidance for staff on the use of Generative AI tools (e.g. ChatGPT) such as not inputting any identifiable information into Generative AI tools and fact checking results to make sure the information is accurate.

- By protecting the Charity from misinformation, disinformation and deep fake from AI via annual risk review conducted by the Director and a member of the board of Trustees.

- By creating a set of 'community rules' for each of our online platforms that allow young people to post and guidance for monitoring these platforms.

Use of photographic and Video images

During induction meetings, parents/carers sign a form verifying that staff have explained photos will be taken during activities for us as evidence for exam board qualifications. Parents have the choice to allow such images to be used in other publicity and social media for the charity in addition to this, but are free to identify that they are only to be used for the purpose of qualifications. Where this is identified, photos are deleted from their secure storage once the young person has finished a qualification and will not be used on social media or publicity at any time.

Communicating with a Young Person Electronically

Communication between children, young people and workers, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mail, social networking sites (such as Facebook and Instagram), digital cameras, videos, web-cams and blogs. In the case of social networking sites, Eagle's Nest is explicit in explaining that no worker should become 'friends' or 'linked' through their personal accounts. Adults should not share personal information with a child or young person. They should not request, or respond to, personal information from the child or young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny (e.g. by always copying another in to all communications where possible).

We recognise that many young people are more comfortable to communicate electronically than they are verbally, and that the use of such facilities aids their positive engagement with us. We have therefore put the following guidelines in place to support such communications in being transparent and safe:

- If a young person is happy to provide their direct phone number, this will always be with the knowledge of the parent.
- Wherever possible, all text or WhatsApp or similar communication will be via one of the Eagle's Nest Project phones, so that no personal staff numbers are made available to students. The exception to this is for the XL-Mentoring project, where specific arrangements are in place as volunteer mentors do not have access to a work phone:

For the first six sessions of a mentoring relationship, all communication must be either via the parents of the mentee or the Eagle's Nest phone. This will help to support clear boundary setting, will develop the trust and relationship with the parents and will protect you whilst the relationship is established and whilst you decide how you would feel comfortable with communication continuing. At the end of the six sessions an agreement can be reached between the coordinator and parents about whether to continue communicating in this way, or to use your personal number to communicate with your mentee.

- Parents/carers are clear about the methods of communication being used and are happy with these. No messages should be deleted from phones as a precaution to safeguard those involved. If concerns arise about inappropriate messages received from the young person (YP), this should be passed to the Designated Safeguarding Lead.
- Any email communication with an under 18 should be copied to another member of the team.
- If young people wish to remain connected during or after their time at Eagle's Nest, they should be encouraged to follow the Eagle's Nest Facebook or Instagram page, and to send messages to this page on messenger, where they can receive a response from Eagle's Nest.
- Staff and volunteers are not allowed to connect with U18 involved with Eagle's Nest on their personal Social media accounts such as Facebook and Instagram.

During induction, parents are given contact telephone numbers and are encouraged to get in touch if they are ever concerned. Regular contact is made with parents throughout periods of engagement to create positive and trusted relationships that foster honestly and openness about concern.

Video calls and using technology for remote sessions

If video calling is deemed to be the most effective method for a remote session with a YP the following guidance should be followed:

- Always message or voice call the YP before video calling to check that they are ready for the call.
- Ask for carer/parent to be present at the start of the call, just to say 'Hi' so that the staff member knows that a responsible adult in the home is aware of the call.
- Video call to take place via WhatsApp, FaceTime, Zoom, or Teams.
- Do NOT use Instagram, Snapchat, Houseparty or any other that keeps no record of the interaction.
- If video call is not the best-suited option at the time, normal phone calls can take place.
- Staff members to be dressed appropriately during virtual meeting.
- Staff to conduct virtual meeting with YP from EN site if possible, or other appropriate spaces/locations.
- Staff to consider imagery in background when conducting virtual meetings.
- Staff to ask YP if there is an appropriate location in YP house/community that they feel comfortable to have the virtual meeting. Please refrain from YP speaking with you in their bedroom.
- When virtual calling YP, if they are dressed inappropriately (e.g., wearing pyjamas, underwear, no shirt etc.), explain that you will have to call back after they get dressed into appropriate clothing. Should this happen, inform DSL/DDSL.

- If staff see drug paraphernalia, alcohol or concerning items in the house if appropriate at the time and based on the level of working relationship speak with YP about it there and then. If not appropriate revisit in follow up meeting. Always inform DSL/DDSL.
- If the YP is under the influence of drugs/alcohol virtual meeting needs to be postponed, with reasons being explained. Follow up meeting to be set up . Always inform DSL/DDSL.

Online abuse

The risks of the internet being used for online abuse is something Eagle's Nest Project takes very seriously. We seek to develop a culture where staff and students are clear this is not acceptable, and where they feel confident to report what has happened.

Any abusive behaviour should be reported to the Designated Safeguarding Lead in the same way that any other safeguarding concern would be. Abuse can be carried out by adults or children over the internet and we recognise that social media in particular, have become a vehicle for child-on-child abuse and that these issues can cause significant distress and humiliation for those involved. If online abuse occurs, we will follow our safeguarding procedures for responding to any kind of abuse, involving outside agencies where required, including CEOP (Child Exploitation and Online Protection Command).

We recognise this may be as a result of a young person or employee disclosing something that has happened out of centre and not directly related to Eagle's Nest, or something that has happened during sessions or is directly linked to their involvement with Eagle's Nest, (e.g. malicious comments made about a young person or employee from Eagle's Nest on social media). In all cases, the matter will be dealt with as serious. Where the case is linked to Eagle's Nest, it is likely that along with following the necessary safeguarding measures, additional support and actions will be needed to ensure all involved and affected are supported to a satisfactory conclusion. It is likely procedures in our Safeguarding, Anti-bullying and/or Behaviour Policy will be drawn upon.

Specific Areas of Concern for Young People

As an organisation, we recognise that there are specific trends that are particularly prevalent at this time, and we must be vigilant to spot these in conversations amongst young people, and to help to educate them about the dangers, passing on concerns in the most relevant way, (see Safeguarding Policy).

Child sexual abuse material (CSAM) including that generated by AI (AI-CSAM)

Sharing of nude/semi-nude images Sharing of nude/semi-nude images (also known as sexting or youth produced sexual imagery g) is when a young person takes an indecent images of themselves and sends this to their friends or boy / girlfriends via mobile phones. The problem is that once taken and sent, the sender has lost control of these images and these images could end up anywhere. They could be seen by future employers, their friends or even by paedophiles. By having in their possession, or distributing, indecent images of a person under 18 on to someone else – young people are not even aware that they could be breaking the law as these are offences. There are significant risks on a number of levels and images can be used to manipulate and coerce further behaviours.

AI produced images

Child sexual abuse material is always illegal, regardless of how it is created. Section 1 of the Protection of Children Act 1978 criminalises the taking, distribution and possession of an "indecent photograph or pseudo photograph of a child" (anyone under the age of 18). It is still illegal, even if the material is not photorealistic.

The use of AI does not lessen the impact or harm caused to victims. The harm to victims is always significant, regardless of the method used to create the CSAM

Upskirting

Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitalia or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm**.**

Viewing Explicit Material

All devices being used by students will be monitored by staff. If a student has refused to hand their personal devices in and is then refusing to allow staff to see what they are viewing, staff must inform parents/carers of this at the end of the session. It is important for parents/carers to know that we do not know what content was viewed in these circumstances, if they have their own data to access the internet.

Pornography

Pornography is the viewing of explicit sexual images and acts, including those produced by AI. Without robust filtering and monitoring security settings in place, the internet makes this much more easily accessible to those under 18s. There is a growing body of evidence that shows the negative effects on relationship values and safe sexual conduct as a result of viewing such material.

Live stream deaths or harm (Suicide or Terrorism)

Live stream deaths have been broadcast using a range of applications, including YouTube and TikTok. These can be either murders linked to terrorism, such as beheadings, or filmed suicidal acts, either linked or unlinked to terrorism. These are clearly highly distressing and traumatic events to view, along with providing the potential for 'copycat' behavior for those struggling with their own mental health issues, (in the case of suicide).

Extremism leading to Radicalisation

Radicalisation is defined in safeguarding terms as the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. These extreme political or social views are often promoted through the use of videos on social media, whereby vulnerable young people are targeted and 'groomed' to develop the belief in order to be drawn into radical behaviours for a specific cause.

This policy is closely linked to the Safeguarding Policy, Anti-bullying Policy, Behaviour Policy and Staff Code of Conduct.