E-SAFETY POLICY

Written by Matt Smith

Date of Last Review 30/08/2024

Date of Next Review 30/08/2026

E-Safety Policy

Here at Beyond Youth Project we realise that it is essential for our children to be safeguarded from potentially harmful and inappropriate online material. We have an effective whole site approach to online safety which empowers us to protect and educate students, and staff in their use of technology and establishes mechanisms for us to identify, intervene in, and escalate any concerns 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;
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Consideration of these 4Cs will provide the basis for our Online Safety policy.

E-Safety Definition

Beyond Youth Project (BYP) 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), Instant Messaging (IM), social networking sites (SNS) and other social media; often referred to as Information and Communications Technology (ICT).

The technology is constantly advancing bringing with it additional safeguarding considerations. An e-safety policy should be adopted and adapted to reflect all communications between BYP employees (staff 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:

- 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. If the staff member is called away whilst a student has access to the internet, the session and device will be logged out and paused until the staff member is back to fully supervise.
- 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 seeking educational opportunities with young people to discuss the appropriate use of the internet and social media.
- 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, 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, sexting, sexual abuse and sexual exploitation.

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 qualifications. Parents have the choice to allow such images to be used in other publicity and social media for the BYP 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/instant 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, BYP 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 provides their direct phone number, this will always be with the knowledge of the parent.

- 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, 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.

- Staff and volunteers are not allowed to connect with U18 involved with Beyond Youth Project 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.

Online abuse

The risks of the internet being used for online abuse is something BYP 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 peer-on-peer 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.

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 Beyond Youth Project, or something that has happened during sessions or is directly linked to their involvement with BYP, (e.g. malicious comments made about a young person or employee from BYP on social media). In all cases, the matter will be dealt with as serious. Where the case is linked to Beyond Youth Project, 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

Sexting (Youth produced sexual imagery)

Sexting 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.

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

Pornography

Pornography is the viewing of explicit sexual images and acts. Without robust 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' behaviour 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, Prevent Policy