# Shoot Academy Online Safety Policy

**1. Introduction**

**Shoot academy are committed to the safety and care of all the young people that we work with. We want to provide compassion, security, and a Gospel-centred approach to all our interactions with young people - in physical reality, or in the digital world.**

**There are inherent problems with a static e-safety policy as new technologies appear almost weekly. However, this document will endeavour to provide a broad and helpful basis for the technologies that we know young people are regularly engaging with. Due to the ever changing nature of digital technologies, it is best practice that Shoot Academy will review this policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.**

**The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with young people ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm. The policy will also form part of the Shoot Academy protection from legal challenges, relating to the use of digital technologies.**

**This policy applies to all volunteers, trustee's and workers of the Shoot Academy community (including staff, volunteers, and young people) who have access to and are users of Shoot Academy systems or Social Media accounts.**

**1**

**1.1 The Place of Email, Mobile Communications, Social Media, Media Sharing Live Streaming & Micro Blogging Apps**

**Interactive social media sites are an everyday part of young people lives. Facebook, twitter, snapchat, Instagram, WhatsApp, YouTube, Tumblr etc. are commonplace online spaces where young people share and interact with personal information, pictures, locations, and opinions.**

**At Shoot Academy, we want to interact with both young people and these online spaces in a healthy and compassionate way.**

**We recognise the inherent benefits of engaging with Social Media and Mobile Communication Technology and plan on always doing so in a safe way.**

**1.2 Safeguarding Risks**

- **Bullying online (cyberbullying)**
- **Posting vulnerable information about young people - including locations and personal details**
- **Sexual grooming, exploitation and abuse**
- **Exposure to inappropriate content, including racist or hate material, or to information or persons that encourage self-harm (including but not limited to drug taking, excessive or underage drinking, cutting, burning, not eating etc.)**
- **Involvement in the creation and/or distribution of illegal and/or inappropriate content**
- **Theft of personal information**

**• Physical harm from recreating, enacting and videoing stunts or other risk-taking activities**

**1.3 Training for Staff and Volunteers**

**A planned programme of formal online safety training will be made available to all volunteers at least annually as part of our mandatory safeguarding refresher. This will be regularly updated and reinforced.**

**All new team will receive online safety training as part of their induction through the volunteer handbook.**

**2. Policy Statements**

**2.1 Data Protection**

**Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:**

**• Fairly and lawfully processed**

**• Processed for limited purposes**

**• Adequate, relevant and not excessive**

**• Accurate**

**• Kept no longer than is necessary**

**• Processed in accordance with the data subject's rights • Secure**

**• Only transferred to others with adequate protection.**

**2.2 Digital and Video Images**

**In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their young people at Shoot events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be made publicly available on social networking sites.**

**Staff and volunteers can take digital / video images to support but must follow policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Shoot Academy equipment, the personal equipment of team should not be used for such purposes without special instructions given by the trustees or director - which should include the transferal to from personal equipment to the charity's equipment.**

**Care should be taken when taking digital / video images that young people are appropriately dressed and are not participating in activities that might bring the individuals Shoot Academy into disrepute. Shoot academy will not post or send content, images, or video that could be intimate, private or hurtful.**

**Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images.**

# Shoot Academy Online Safety Policy

**Young people's full names will not be used anywhere on a website or blog, particularly in association with photographs**

**2.3 Communications**

**The official Shoot Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. The Facebook account should be managed and monitored by multiple members of team. All comments made on any uploaded or shared material Shoot Academy is responsible for will be carefully monitored.**

**Any digital communication between team and young people (email, social media, chat, blogs, etc) must be professional in tone and content.**

**4**

**All accounts associated with Shoot Academy should be identified as such by using the charity brand 'Shoot Academy'.**

**When at all possible, interactions on Social Media will be public. Shoot Academy will not use private messaging spaces if possible, on social media. Also, the same confidentiality agreements stand as in-person interactions (i.e. Shoot Academy team members cannot guarantee confidentiality).**

**Shoot Academy will not target underage children for communications online (being aware that different Social Media sites have different age policies).**

**Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with Shoot Academy or impacts on Shoot it must be made clear that the member of staff is not communicating on behalf of Shoot Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy. Shoot Academy will not use private email accounts for any professional communication with young people (under 18).**

**Shoot Academy team will not accept young people (under 18) as friends on personal accounts or 'follow' young people on sites/apps like Instagram or Snapchat from personal or charity accounts.**

**2.4 Unsuitable / Inappropriate / Illegal Activities**

**Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from all Shoot Academy technical systems and accounts. Other activities e.g. cyberbullying is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would still be inappropriate in Shoot Academy projects, either because of the age of the users or the nature of those activities. These include, but are not limited to:**

**5**

- **Pornography**
- **Online gambling**
- **Promotion of any kind of discrimination**

**• Threatening behaviour, including the promotion of physical violence or mental harm**

**• Promotion of terrorism or extremism**

**• Any other information which may be offensive, or breach the integrity of the ethos or mission of Shoot Academy, or brings Shoot Academy into disrepute**

**• Using the Shoot Academy systems or accounts to run a private business**

**• Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy**

**• Infringing copyright**

**• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)**

**• Creating or propagating computer viruses or other harmful files**

**• Unfair usage (downloading / uploading large files that hinders others in their use of the internet)**

**2.4.1 Illegal Online Activities In the event of suspicion of illegal activities, all steps in this procedure should be followed:**

**1. Have more than one senior member of staff / volunteer / trustee involved in this process. This is vital to protect individuals if accusations are subsequently reported.**

**2. Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.**

**3. It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).**

**6**

**4. Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).**

**5. Once this has been completed and fully investigated the group will need to judge this concern has substance or not. If it does, then appropriate action will be required and could include the following:**

**5.1 Internal response or discipline procedures 5.2 Involvement by Social Services 5.3 Police involvement and/or action**

**6. If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

**• incidents of 'grooming' behaviour**

**• the sending of obscene materials to a child**

**• adult material which potentially breaches the Obscene Publications Act**

**• criminally racist material**

**• promotion of terrorism or extremism**

**• other criminal conduct, activity or materials**

**7. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

**It is important that all the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.**

**7**

**2.4.1.1 Awareness of Legal Offences and Consequences There are offences that can be committed over social media, email, mobile technology and interactive internet spaces. These include, but are not limited to:**

**• Threats of violence or to kill**

**• Threats to property**

**• Intended harassment or to cause distress, or anxiety**

**• Causing intended harm of distress**

**This (depending on convictions of summary or indictable offences) can range from a fine to 10 years in prison.**

**2.4.2 Inappropriate Online Activities It is more likely that Shoot Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows (depending on the activity in question and offending person):**

**• Referral to Social Services**

**• Referral to Police**

**• Referral to parents / carers**

**• Referral to school • Referral to Director**

**• Referral to Trustees / Chair**

**• More action regarding technical filtering or accountability**

**• Removal of network, internet rights**

**• Removal and blocking from social media page, group or forum**

**• Warning**

- **Banning or suspension from project attendance**

**8**

**3. Reporting Breaches of Policy**

**Where a young person may be in immediate danger, dial 999 for emergency assistance.**

**Report all concerns to a member of the Shoot Academy Safeguarding Board - as laid out in the main Safeguarding Policy. This board includes the Director, Safeguarding Administrator, Chair of Trustees, and Designated Safeguarding Officer.**

**January 2020**

**(To be reviewed July 2020)**