YOUTH
FOR CHRIST

Online Safety Policy

Online safety is the collective term for safeguarding involving the use of electronic devices and applications to communicate and access the internet; often referred to as Information and Communications Technology, including online gaming platforms, livestreaming services and community servers. This policy covers the safe use of such technology by children, young people, trustees, staff and volunteers in any context under the auspices of Youth for Christ, either nationally or in local contexts.

As a Christian organisation, Youth for Christ affirms our belief in the God-given value of every individual with whom we work or have contact. In recognition of God's wholehearted commitment to them, we are committed to treating each individual with value and dignity and aim that no one suffers abuse of any kind.

It is the responsibility of each one of us to safeguard children, young people, and adults with additional care and support needs against any form of harm and to report any abuse discovered or suspected, both online and offline. With this in mind, Youth for Christ is committed to supporting, resourcing and training all those who work with children, young people, and adults with additional care and support needs across our ministries.

This policy is for use by both national team (British Youth for Christ) and chartered local ministries (local centres or projects) operating as part of Youth for Christ in England, Scotland and Wales.

If there are any breaches or concerns that arise regarding online safety, then Youth for Christ will follow their Safeguarding Policy and Procedures to address these concerns appropriately.

The British Youth for Christ Board shall review this online safety policy on an annual basis in September, and any updates or revisions to the policy will be sent out to all local ministries before the end of September of each year for adoption.

National Safeguarding Officer: Lesley Taberer - 07890 414236
National Trustee with Safeguarding Responsibility: Annabel Wheeldon-Clarke
Local Centre Safeguarding Officer: Tim Wye-Williams – 07825 346746
Local Centre Trustee with Safeguarding Responsibility: John Stewart

Responsibility for the implementation of this policy lies with the relevant trustees, but some aspects may be delegated to others. Workers refer to all those who work for Youth for Christ in either employed or voluntary roles. This policy should be read in conjunction with our Safeguarding Policy and Code of Conduct.

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England, Northern Ireland, Scotland and Wales. The key legislation and guidance for this policy can be found under the Sexual Offences Act 2003, Online Safety Act 2023.

a) General Principles

Trustees of Youth for Christ or those delegated responsibility will:

- Exercise our right to monitor the use of all our systems with internet access. This will include access to websites, the interception of e-mail and the deletion of inappropriate material where we believe unauthorised use of the computer system is or may be taking place, or the system is or may be being used for a criminal purpose or for storing unauthorised or unlawful text, images or sound.
- Ensure that unwanted/unsolicited information, viruses and other malware do not intrude on the use of IT.
- Ensure all appropriate and reasonable steps are taken to protect computers and the users of them.

Workers will:

- Ensure all use of IT is carried out with integrity, appropriately and within the parameters of this policy and the British Youth for Christ Code of Conduct.
- Ensure that all online communication is clear and appropriate to the context and purpose, and is open to scrutiny.
- Be circumspect in all online communications with children, young people and adults with additional care and support needs, to avoid any possible misinterpretation.
- Only give personal details to children, young people and adults with additional care and support needs that are within the public domain and appropriate to the context.
- Only make contact with children, young people, and adults with additional care and support needs for reasons related to their work and maintain a log of all electronic contact with individuals or groups.
- Only use Youth for Christ equipment to communicate for work purposes with children, young people or adults with additional care and support needs (i.e., not personal equipment) unless previously agreed with trustees or delegated manager.
- Only use agreed methods of communication, approved by trustees or delegated manager, and parents/carers.
- Respect a person's right to confidentiality unless abuse/harm is suspected or disclosed.
- Ensure Youth for Christ's domain name/logo appears with every internet post made by a user in the context of their connection to Youth for Christ. Any user may thus be viewed as a representative of Youth for Christ while conducting business on the internet. No anonymous messages should ever be sent in the work context.
- Inform parents/carers of intended methods and context of communication and the rules for appropriate use of Youth for Christ equipment and internet use by both workers and children, young people or adults with additional care and support needs. If the parent/carer requests that their child not be communicated with in a certain way, this must be respected and an alternative found.
- Refer all safeguarding concerns/allegations arising from online communication to their safeguarding officer.
- Only communicate with children, young people or adults with additional care and support needs and their parents/carers during reasonable working hours except in emergency circumstances or where there is a potential risk of harm. Communication with children and young people should be done within agreed, reasonable hours, for example, taking into account an appropriate bedtime for that age and should not take place outside of these times, except in emergency situations.

b) Acceptable Use

When using a computer or electronic device with internet access on Youth for Christ premises, at a Youth for Christ event and/or using Youth for Christ equipment, workers are not permitted to:

- Search for and/or enter inappropriate websites, including pornographic, racist or hate-motivated content.
- Send, display, retrieve or copy offensive messages or pictures unless handling this information is for specific safeguarding/reporting purposes.
- Use obscene language.
- Violate copyright laws; i.e., illegally copy or play copyrighted content where permission has not been given.
- Trespass in others' folders, work or files (i.e., enter without permission).
- Harass, insult, bully or attack others.
- Damage computers, computer systems or computer networks.
- Use another user's password.
- Use equipment or devices without relevant permission or add software without permission.
- Use computers for unapproved commercial purposes.
- Access, download, send or receive any data (including images), which are considered offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

In addition, workers must report anything that is seen or received which may be unsuitable, offensive or which contravenes any of the rules outlined in the policy. Violation of any of these rules could result in disciplinary action being taken in line with Youth for Christ's disciplinary policy. When applicable, police or local authorities will be informed.

Responsible use of equipment belonging to Youth for Christ and the appropriate use of the internet at Youth for Christ activities should also be included on general registration and/or consent forms so that parents/carers understand the rules above and agree that children, young people and adults with additional care and support needs are also subject to these rules whilst participating in activities.

Whilst it is not possible to legislate for how a child, young person or adults with additional care and support needs uses their personal devices, it should be clear that violations of the above rules will have consequences. Serious violations could include a temporary or permanent ban from the activity or group and information being passed onto their parent/carer, the police or other statutory agencies. Some violations could include a ban on the use of Youth for Christ equipment or other appropriate sanctions, determined by the local context.

c) Social Media

Workers will:

- Not use a personal account, in preference to specifically established group accounts or an individual work account, for the purpose of communicating via social media and therefore not add any children, young people or adults with additional care and support needs to their private personal social media.
- If workers do have personal profiles on social media, workers should ensure that their profiles are set to the highest level of security and privacy to avoid unauthorised access and communication.
- Not share personal information with a child, young person or adults with additional care and support needs.

- Ensure that administrative details are not shared with children, young people or adults with additional care and support needs.
- Limit interaction with children, young people, and adults with additional care and support needs to monitored/administered groups.
- Ensure that all text and any other media posted shall be subject to the acceptable use rules above.
- Record all interactions on social media groups for safeguarding purposes.
- Only use private messaging in emergency circumstances and never use any non-recordable private messages
- Ensure all users of social media are above the relevant minimum age limit (i.e., 13 for Facebook, 13 for WhatsApp).
- Ensure their privacy settings offer the highest level of security in order to restrict children or young people from being able to see any more than what is relevant to communication within the group.
- Provide links on social media groups to statutory authorities such as the Child Exploitation and Online Protection (CEOP) Centre, to enable children to report online abuse.
- Encourage children, young people and adults with additional care and support needs to use social media responsibly and safely. More advice for charities and their use of social media can be found at Charities and social media – GOV.UK - https://www.gov.uk/government/publications/charities-and-social-media/charities-and-social-media

d) Email Communication

When communicating via email, every effort should be made to ensure that the method of communication is secure (eg only sending email to sure addresses), only accessed by the appropriate person (blind copy function should be used so as not to disclose email addresses to a wider group where not appropriate) and that minimal identifying detail is included where security cannot be guaranteed (eg using initials rather than full names).

When using email to communicate with children, young people or adults with additional care and support needs, workers will:

- Ensure all emails are transparent and open to scrutiny. This means they could be viewed at any time by a supervisor or trustee. (Where necessary, this should be explained to children and young people, in the same way that confidentiality is not promised in other contexts.
- Obtain parental agreement before they use email services to communicate with a child or young person.
- Use clear, unambiguous language to reduce the risk of misinterpretation.
- Not give their personal contact details to children or young people, including details of any blogs or personal websites, unless these are agreed forms of communication.
- Retain secure records of email communication with children, young people and adults with additional care and support needs, which should be dated.

e) Mobile Phones

A worker should be supplied with a work-dedicated phone. This way, all calls and texts can be accounted for via an itemised phone bill. It also protects the worker's right to a personal life outside work and offers a greater level of accountability and transparency for all concerned.

Where this is not possible, or the work phone is not working or is otherwise unusable, then the worker may use a personal phone for work purposes, within parameters which are agreed in advance with their trustees or delegated manager.

Workers will:

- Ensure all texts and records of phone calls are transparent and open to scrutiny. This means they could be viewed at any time by a supervisor or trustee. (where necessary, this should be explained to children and young people in the same way that confidentiality is not promised in other contexts).
- Be clear to children, young people and adults with additional care and support needs about their normal working hours and when they can be available to speak to on the phone or respond to texts.
- Not divulge their personal mobile number unless to ensure contact can be made in exceptional circumstances. These should be reported.
- Use group text rather than texting individuals. Any texts to an individual should be avoided, but where necessary, should either be copied to an appropriate colleague or trustee, or otherwise kept and recorded.

- Ensure they use clear, appropriate and unambiguous language and be cautious about the use of emoticons, which could be misinterpreted.
- Ensure that any texts or conversations that raise concerns are saved/recorded (either literally or notes made immediately following a conversation) and reported to the workers' supervisor.
- Only make contact via text or mobile calls during set appropriate hours and only for work purposes.
- Enable a password/lock on their phone for data protection and not allow unauthorised access.
- Ensure that they only take photographs of children and young people on their phones in accordance with the guidelines on photography (in section g) and should not retain copies of images on their work phone, unless previously agreed with their line manager and permission given by parents/carers for this practice. They should never take or store photos of children or young people known through work on their personal phone, unless this is being used in an emergency and photographic evidence needs to be recorded and transferred to a work-approved device at the earliest opportunity.

f) Chat and Messenger Services

Instant or Direct Messenger Services (IM/DM) are programmes that allow people to write and receive messages in real time and are often used by children and young people for one-to-one or group conversations. The same protocols for workers communicating via email and mobile phones also apply to IM/DM; care needs to be taken with regard to language and content, as well as when and for how long a communication lasts.
Workers should ensure that all communications using IM/DM services adhere to the rules above relating to appropriate hours for communication, saving and recording communication and ensuring communication is appropriate and open to scrutiny.

Workers must ensure that they enable settings when using IM/DM services which allow for conversations to be saved as text files and should never use programmes or apps which do not allow conversations to be saved. Children, young people and parents/carers should also be made aware that conversations may be recorded and kept on file.

In gaming and livestream contexts, communication may occur in group voice or text spaces that function differently from traditional messaging services. The safeguarding principles of transparency, accountability and appropriate boundaries still apply, and are implemented through moderation and platform controls rather than private messaging management.

Livestream chats and chat servers must have moderators assigned. The purpose of the moderator is to keep the environment safe by blocking inappropriate messages, issuing warnings and banning people from streams or chats if there is a failure to comply with the rules of the space.

g) Photographic Images and Film

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person should always be sought before an image is taken for any purposes. Where images are to be used in any form of publication (including online), express permission must be sought from parents/carers. Clear guidelines must be followed when using images of children and young people, and these guidelines apply to all content, be it still photographs, films or audio clips, which count as personal data. The following rules apply:

- Workers will ensure there is permission from parents/carers and, where appropriate, the child or young person themselves before any images are taken or displayed.
- Written consent will specify what purposes the image will be used for and how it will be stored. Images will only be used for the specific purposes agreed.
- Written consent will be stored securely, and notice given to those responsible for taking images where consent is not given or withdrawn. Workers are responsible for knowing where permission is refused, withdrawn or otherwise not given and will respect this for the relevant child or young person.
- Any worker will be able to justify images of children or young people in their possession using the above clear purpose, and no images will be taken for personal use or on personal devices.
- Workers will ensure that children and young people understand why the images are being taken.
- Any streams or videos posted online can be permanent, so everyone streaming or uploading content needs to behave in line with the Code of Conduct.
- No pictures or film should be taken when anyone is not appropriately dressed or is in any vulnerable situation (unless using as photographic evidence of an injury or abuse).
- Photographs will not enable individual children to be clearly identified, unless specific permission has been given for use.
- Children's full names will not be used anywhere in association with photographs, without permission.
- Use of images will reflect the diversity of age, ethnicity and gender of the activity.
- Live streaming of events must be clearly advertised in advance and where children are involved, permission should be sought in line with the photographic guidelines.
- There will be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.
- Messages and communication that could be misleading, misinterpreted, personal or sexual must not be sent.

h) Indecent Images

Accessing, making and storing indecent images of children is illegal. This will lead to a criminal investigation and the individual being barred from working with children and young people, if proven. Workers should ensure that children and young people are not exposed to any inappropriate images or web links, and will ensure that all IT equipment and devices used have the appropriate controls with regard to access, e.g., personal passwords should be kept confidential. Where indecent images of children or other unsuitable material are found, the process for reporting concerns outlined in the Safeguarding Policy should be followed. More information can be found to support those who have seen online abuse or inappropriate content: Reporting online safety concerns – NSPCC.

l) 'Sexting' or Cyberflashing

Sexting refers to sending or receiving indecent or inappropriate images, which can be sent to or from a friend, boyfriend/girlfriend or stranger, and although it usually refers to sending via text message, they can also be sent via email, in instant messages or in social media apps, etc.

All workers should be aware of the implications of this behaviour. While the age of sexual consent is 16, the relevant legal age in relation to indecent images is 18. It is therefore:

- Illegal for anyone under 18 to send such an image to anyone else, including if the image is of themselves and sent to a 'partner'.
- Illegal for anyone over 18 to send such images to anyone under 18.
- Illegal for anyone of any age to forward on or publicise such images from other people, in any context.
- Illegal for anyone of any age to possess, take, make, distribute or show anyone an indecent image of anyone under 18 years of age.
- Illegal to send an intimate image of someone without their consent.
- Illegal to send an explicit image to cause the recipient humiliation, alarm or distress.
- Not illegal if sent between consenting adults (but could be considered harassment if unwanted).
- Not illegal if images of an adult are sent between under 18s (but could be considered harassment and may be referred to social services).

In any of the above contexts, if a worker observes or suspects this behaviour in others or if this relates to their own behaviour, then this must be reported to their line manager or Safeguarding Officer.

Workers should:

- Never view, copy, print, share, store or save the imagery themselves, or ask a child to share or download.
- If the worker has already viewed the imagery by accident, report this to the designated safeguarding lead and seek support.
- Never delete the imagery or ask the young person to delete it.
- Not share information about the incident with other members of staff, the young person it involves, or their or other parents and/or carers.
- Explain to the individual that this will need to be reported and reassure them that they will receive support and help from the safeguarding lead.

Additional guidance on responding to instances of sexting can be found at sharing nudes and semi-nudes: how to respond to an incident (overview) (updated March 2024) - GOV.UK (www.gov.uk)

If workers have ongoing concerns about a platform, they can make a complaint to Ofcom. While Ofcom cannot respond to individual complaints, this information can help them to assess which services are complying with the regulation - complain about harmful content on a website or app - Ofcom.

J) Video Chat

Webcams and phone cameras, which allow for the use of programmes such as Zoom, Google Meet or Facetime mean that individuals or groups can contact one another in real time by using 'video calling'. These applications are ideal for one-to-one calls or group contacts, where face-to-face meetings are not possible but the same rules must apply, as if meeting physically face-to-face.

Virtual meetings must adhere to the same rules regarding appropriate boundaries, consent, recording and reporting as would be expected from any other meeting or communication outlined above. Workers should be cautious about making or receiving video chat requests without prior notice, planning or approval and only accept these in exceptional circumstances.

Therefore, workers will:

- Ensure that relevant permission has been sought for any one-to-one video chat context with a child or young person, from their supervisor and from the child's parent/carer. This should be treated the same as a one-to-one meeting context.
- Consider whether group communication can be achieved, rather than a one-to-one. Where appropriate and possible to do so, include two approved workers on the call with an individual young person or a colleague in the room with the worker.
- Ensure that on one-to-one calls, children, young people and adults with additional care and support needs are asked whether a parent can be at home at the same time as the call is occurring.

- Ensure that parental permission is given for group video chats, including the purpose, dates, times and locations for those involved. It is possible to seek consent for regular, ad hoc video chats by outlining the purpose and appropriate boundaries and ensuring these are adhered to.
- Ensure that video calls are password-protected to prevent unintended individuals from entering the call.
- Ensure that the ability to mute and ban individuals on video calls and that screen sharing is restricted.
- Ensure that video calls are not recorded unless there is a compelling reason to do so, and with parental consent in writing. Wherever this is required, calls should be stored safely and password protected.
- Ensure that all video calls are made at times which are appropriate to the context and age of the child.
- Ensure that any participants in a video call are in appropriate locations. This means that all parties are aware of each location and are appropriate for each person. For example, a child or young person should not be anywhere they would not normally allow the worker, such as their bedroom. It is appropriate to find a quiet location, but this should remain fitting for the context and appropriate boundaries should be maintained.
- Ensure that children and young people understand the risks and dangers of this context, and that it is a safe environment to engage in with strangers.

K) Gaming Ministry

When engaging with the Gaming ministries, this specifically applies to online, gaming and livestream contexts, including Discord, Twitch in-game chat, and all other online communication.

Workers will:

- Not engage in one-to-one private digital communication with children or young people.
- When playing specific games with young people or 'playing with viewers', and in-game friendship requests are required, please first seek approval from your line manager and discuss how this safeguarding policy will be applied, e.g., games should only be played when there are two adults available. Consider using specific work accounts for this or how to manage a child joining your game when not working e.g. playing a game online and a child joins your game, you must leave the game immediately and inform the Safeguarding Lead or their deputy as soon as possible.
- Ensure all online interaction takes place through approved platforms and systems, which allow oversight and accountability (including Discord and Twitch)
- Ensure all staff and volunteers maintain a professional tone and behaviour in voice and text chat, recognising that humour, banter or frustration can be misinterpreted online.
- Ensure that all livestreams and gaming sessions must be moderated appropriately, with more than one approved adult present where young people are involved.
- Not direct message any young people.

- Be mindful that online content may be recorded, shared or taken out of context
- Report any concerns arising from online interactions to the Designated Safeguarding Lead.
- Ensure all accounts used to represent the ministry align with this policy, the Safeguarding Policy and the Code of Conduct.
- Adhere to relevant platform Terms of Service (TOS), including minimum age requirements, and must not assume a child's age based on voice, maturity or gameplay. Any concerns regarding a child's age must be escalated to the Designated Safeguarding Lead or their deputy.
- Moderate appropriately and responsibly and not use their authority to manipulate, shame or intimidate any young person.
- Ensure all safeguarding or behavioural concerns are properly reported, logged and escalated as required.
- Adhere to digital conduct expectations, and any failure will be treated as a breach of this policy and the Code of Conduct.
- Remain vigilant and accountable in all digital interactions, recognising that boundaries, tone and authority may be experienced differently online. Where uncertainty exists, safeguarding concerns must always be escalated rather than managed in isolation.
- Be aware and remain vigilant that community servers can be abused by online predators who may post as young people but are looking for the opportunity for grooming/sexual exploitation. Appropriate safeguarding measures should be put in place to reduce this risk.

Where a worker has concerns that guidance in this policy has been breached, in addition to referring to the Safeguarding Policy, workers must:

- Share any concerns with their Safeguarding Lead if they believe that any individual may be at risk of harm.
- Report any breaches or concerns of this policy to the Safeguarding Lead to assess the concerns for next steps.

Concerns raised about a worker's conduct in relation to Youth for Christ Online Safety Policy may result in

- Warnings or disciplinary action in line with existing practice as detailed in the British Youth for Christ Code of Conduct and Disciplinary policies.
- Where applicable, police or local authorities may be involved.

Policy approved September 2026