HOLY TRINITY COVENTRY

Online safety and social media policy

Introduction

The aim of this online safety and social media policy is to protect all children and young people involved in any way with Holy Trinity Church Coventry, who make use of social media and technology. As well as setting out best practice guidelines to safeguard staff, volunteers, and young people alike. This policy should also help ensure that all communications are transparent and open to scrutiny and maintain good relationships with parents and carers regarding communication with their children. And ensuring we operate in line with the law and our values as Christians whilst online. This policy should be used to support the parish safeguarding policy and is under the review of the Parish Safeguarding Officer.

Rationale

Information and communication technology are very much part of our everyday lives. Families are now more connected to the online world than ever before; for children and young people in particular it is the norm to communicate electronically. Because of this, adults who work with children and young people need to be aware of how to make the best use of these technologies, whilst making sure that they are being used appropriately and responsibly. This ensures that children and young people are protected and that workers are safeguarded.

Potential Safeguarding Risks

As with all technology, there is potential for abuse. Risks associated with this technology include:

- Cyberbullying
- Grooming and potential abuse by online predators
- Exposure to inappropriate content including racist and self-hate content and pornography
- Privacy issues with the posting of personal data that can identify and locate children/young people who are potentially at risk
- Privacy issues associated with adults posing as young people and contacting other young people
- Inappropriate contact with young people by a trusted adult.
- Extremist and radicalised material.

However, the answer to abuse is not to avoid using technology but to use it safely, by having clear and appropriate procedures and policies we can ensure these technologies are used safely and effectively.

General Guidelines

It can be helpful to see electronic communication as an extension of general life, you should always follow best practices whether online or in person, for instance, you should not be alone with a young person in a private place. The same still holds true online: Don't have private one to one conversations. Have clear boundaries when communicating with children and young people. Remember that the law and diocesan policies around safeguarding apply in your communications with children and young people – you should not exchange private messages with young people via social media. At Holy Trinity Coventry it was our policy to not use social media or other forms of electronic communication with children under secondary school age. However, in light of COVID, we have decided that it is useful to be able to use social media as an additional form of communication, guidelines for which can be found below.

Parent/Guardian Consent

- No form of electronic communication should be had with a young person without parental/ Legal guardians' consent.
- Parents/Guardians will be kept informed about how and why we use various forms of social media and electronic communication.
- This policy will be made available to parents and legal guardians.

- The asking of consent will take place once a year, most commonly at the start of an academic year, by way of a consent form or by letter with a return slip.

Accountability and Record Keeping

Personal data is stored in line with Holy Trinity's Privacy Policy.
Just like other forms of communication and interactions with young people, a record of the electronic information should be kept in order to protect the young person and safeguard the worker.

- All messages and posts should be kept i.e., not deleted from the server or website once read so that where needed they can be recalled.
- Where it is not feasible for messages and posts to be kept on the site, whether due to lack of storage or for some other concern, a copy should be kept in accordance with GDPR and the data protection policy.
- Those social media platforms unable to offer this level of safeguarding (e.g., Snapchat) will not be used as a form of communication between workers and young people.

General Guidelines whilst online

- The law views anything you share online as being in the public domain.
- Be mindful of your own security. Be careful about the personal details you share online – again, assume anything you share about yourself is in the public domain.
- Assume that what you say is permanent.
- Do not assume anything electronic is secure, private, or confidential.
- Being in a position of leadership/ authority, we should be careful with how we use electronic communication, it should be primarily for work not for general socialising.
- It is up to you to ensure any hyperlinks do not lead to inappropriate or dangerous material.
- Be aware of your privacy settings and who can see what you post/ say online.
    - If you are unsure of who can see it is best to assume it is public.
    - You should also be aware that host privacy settings often change and as such you should keep track of yours.
    - We also highly recommend that you set permissions so that young people cannot see when you are online, or "available to chat".

- Ensure you have adequate security on all your devices i.e., password and pin.
- Ensure all information that is publicly available about you is accurate and appropriate (i.e., being a good witness).
    - This includes photos and posts you may have posted or been tagged in.

Guidelines around messaging

- The language used should be clear, and professional; avoid using text speak, abbreviations ("lol" can mean laugh out loud or lots of love for example), Emojis, or terms of affection i.e., luv, xxx etc.
    - Nuance and tone can also be hard to read, as such ambiguity, flirtation, crude humour and ridicule or insulting language should not be used even in jest.
- Do not say anything you wouldn't say face to face.
- Try to keep all communication public where appropriate, and to groups rather than to individuals.
    - Where it is not appropriate to message publicly or to a group, another adult (parent/guardian, or another leader) must be included in the message.
    - Please also consider whether this might be better discussed live either face to face or via a phone conversation.
- It is advised that all messages should take place during office hours where possible and not after 9:30 pm or before 7:30 am as this can be considered an intimate act, unless absolutely necessary.
    - Do not contact a Child or Young Person unless you would be happy to meet face to face at that time.
- Think carefully about sending images, it is generally better to avoid this as it may set an unhelpful precedent. Any images you do choose to send must comply with the Churches Photography and images policy.
    - You should not send Images that are of just you as this can easily be misconstrued.
- Remember the value of other forms of communication! It can become very easy to hide behind an online persona and neglect other relationships – remember that while social media is an exciting forum which presents many new opportunities, the value of face-to-face relationships should never be forgotten.

- We must also ensure that those who do not have access to various forms of electronic communication or whose parents/guardians do not allow communication in this way do not miss out on information or become excluded because of this.

Guidelines around disclosures and boundaries

- Any disclosures of abuse reported online or through social media must be treated in the same way as a face-to-face disclosure.
  - If a disclosure is made to you directly i.e., via text or email you should try and contact them via another means of communication ideally in person. However, it is more important that the young person feels comfortable enough to make the disclosure, it might be that they only feel comfortable disclosing initially through writing, once they have finished disclosing in this way safeguarding policy must be followed, i.e., ensuring they are not in immediate harm, and arranging support.
- As with all face-to-face meetings, a record should be kept of when communication is exchanged, and in the case of written communication, a record of what all parties have written should be kept.
  - Apps or websites that delete messages once they have been read should not be used i.e., Snapchat
  - Zoom, Skype, Facetime and other video chat services should not be used for 1-1 communication as this can be considered intimate and inappropriate, the exception being a conference or group call.
- You are encouraged to stop a conversation if you feel uncomfortable with the content or topic and should encourage them to either resume the conversation the next time you meet or explain why you feel uncomfortable and potentially point them in the direction of someone, they can continue the conversation with.
- You are accountable for reporting any inappropriate conversation (such as a young person being overly familiar, or flirtatious) to a supervisor or safeguarding officer.
  - This also holds true for conversations that raise concerns, it should not be dismissed just because it is online.
- As with face-to-face contact, do not allow one or a few young people to monopolise your time.

Specific guidance

No matter what way we choose to communicate we must do so in accordance with the guidelines set out above, however, each means of communication needs to be thought about in its own right, as such we have included some more specific guidelines for each form of communication we currently use.

Email

- Should only be used for the sending out of Information and not for relationship building.
- Only use a specific work email rather than a personal one, when contacting young people.
    - Where it is possible for the line manager to access the account.
- All emails involving young people and or their parents/guardians must be kept.
- Emails should be used to communicate with groups rather than individuals.
- Do not forward chain emails, email petitions, or anything else that might be unwanted or thought of as spam.
- If a Disclosure is made via email the young person should be contacted via another means of communication ideally in person. And all other standard safeguarding policies should be followed.

Text messaging

- Text messaging is not a preferred means of communication due to difficulty in keeping accountable.
- Messages should ideally be sent to both parents/guardians and children.
    - If it is not appropriate for any reason to message a parent/guardian and child another leader must be included.
- Copies of messages must be kept, in accordance with our record keeping policy.

WhatsApp

- Staff and volunteers may use WhatsApp group messages with young people where all the participants are staff, volunteers, children and young people or parents/guardians; there must be at least two adults in each message.

- As WhatsApp shares members' phone numbers, it is important that parents/guardians are made aware of this fact when we ask for parental/legal guardian's consent.

Facebook

- “Friend Requests” from young people can be accepted with due consideration, provided they are old enough to use the platform (13 for Facebook currently).
- If you choose to accept friend requests from those under 18 you should ensure that the content of what you post (and may be tagged in) is appropriate, and or would not cause you to fall into disrepute.
    - You are a role model (and it is likely that young people will look up to you as an example of what it looks like to be a Christian) and should act with this in mind.
- The sending of friend requests to under 18’s is discouraged, it is better that they add you.
    - Exceptions being when you have regular contact with parents/ guardians of the said young person i.e., a family friend.
    - You also should not pressure or tell young people to add you, this must be their own decision.
- Any groups set up on Facebook for youth work must adhere to the points under public accounts.

Instagram

- If leaders choose to use Instagram, they should not use the messaging feature as they are direct messages that are hard to back up.
- any images posted must follow the photography and video policy.
    - As well as following photography and video policy leaders should be aware that they are role models and should post accordingly.
- Leaders are free to choose whether or not to have their profile private or public.
- Following young people is permitted if they have a public profile, if it is set to private however it is up to them to follow you if they wish, then follow backs are permitted.

Twitter

- The public nature of the majority of Twitter profiles means that young people can freely choose to 'follow' you on the platform.
- You are permitted to freely choose to 'follow' young people, as long as their profile is public, if it is set to private you are only permitted to follow them if they first follow you.
- As with other sites, you should not use the direct messaging function.

Skype, Zoom, Facebook messenger, and other video conferencing sites

- Invitations to join these groups will be made to parents' email addresses stating the details of the event including how long the event is going to run and which leaders are going to be part of the group. It is through this link that young people can be a part of the session.
- Leaders should be ready and waiting on the group before the young people arrive, as per a face-to-face meeting.
- All leaders must have DBS and there must be at least two leaders involved in a session.
- Young people should be in a shared family space whilst in the session (e.g., living rooms/dining rooms not in bedrooms).

Phone calls

Should parents want us to, we are willing to have phone conversations with young people. When phone calls are made a parent/ guardian should be called first and asked to pass the phone and then passed back to the parent/ guardian when the call is finished, so they are aware of when the phone call is going on. Alternatively, parents may prefer to be in on the phone call and can choose to put it on speakerphone. The general policy will still be followed i.e., times of calling etc.

Additional guidelines for using social media with primary aged children

- Communication with children of primary school age should be in response to parents/guardians' requests unless there is a need to move regular groups online (e.g., COVID lockdowns).
- We will not make any form of contact with a primary school aged child, however, if parents/ guardians should ask for assistance we will endeavour to provide support, following the general guidelines of our social media policy.
- All forms of communication will be made first to parents/ guardians who will then put on the child, when the communication is finished, the child will be asked to put the parent/ guardian back on when the communication is finished so they are aware of when the communication is going on.
- Alternatively, parents may prefer to be a part of the communication and can choose to stay involved i.e., using speakerphone.
- As always records must be kept as to when communication is made.
- As all communication will be going through parents/guardians we can use those conversations as consent rather than needing a signed consent form.

Public accounts

Any accounts set up to be a face for Youth or children's work at Holy Trinity Coventry

- Profiles and accounts must be password protected with at least 3 members of staff/ volunteers having access to each account.
- The account must be administered by an appointed leader, who will remove any inappropriate posts made by young people or others, explain why it has been removed, and inform any parties involved (including parents/ guardians of any young people involved).
- No identifying or contact details should be posted for or about young people.
- Posts should be signed by whoever posted them using the account, so young people know who they are interacting with.
- Posts should ideally be limited to providing details and publicity for events.
- Any Groups/ pages must be administered by at least two leaders ideally more, and must not be secret or hidden (it should be clear who is a member of any group), however, they can and often should be private so that only members can see their content.
    - Events at a private address must only be posted in private groups.
- Direct messaging should be disabled where this is possible and not used where it is not possible to be disabled.
- Use of any images, or video must adhere to the photo and video policy.

Online Gaming

Due to the vast amounts of different gaming websites, applications and platforms rather than, trying to provide a policy for each and every one that we may wish to use this policy will aim to provide criteria to determine whether or not a particular online game or the like is suitable for use (here on these will be referred to as apps, regardless of whether they are entirely browser based or have standalone apps). In addition to the parameters set out in this document, each site will need to have a risk assessment made to address any specific risks a particular site may pose.

Requirements

- All apps must be able to host a private group, ideally requiring a code or password to join.
- As with all that we do the apps we wish to use must be age appropriate.
- If an app's policy only permits use by those who are aged 13+ for example then a parent/guardian must create an account, on behalf of anyone under that age, this will be at parent/guardians' discretion.
- Any app must not rely on a text-based chat, ideally, any site will either; not provide a text chat, or have a way of turning off text chat, but where this is not possible there must be a way to record this chat. Those involved must be made aware that the text chat will be recorded if they choose to use it and it should be recommended that they do not use it.
- Any app must not allow for 1-1 messaging.
- As far as possible any apps used must be accessible to multiple platforms, we must aim to be as accessible as possible.
- As stated earlier all apps require their own risk assessment.

Should it be deemed necessary specific parental/ guardian permission should be sought (for example if a site shares additional information, like WhatsApp allows others to see the member's phone numbers), otherwise a generic gaming/ social media tick-box on the yearly consent form will suffice.

Ideally

- Any app should not require users to create an account.
- Any app should not need to install anything, again ideally it should be entirely web browser based or, like zoom, for instance, have applications for multiple platforms.

Cyberbullying Guidelines

Cyberbullying is bullying and must be treated as such. We should not treat it differently than any other form of bullying, with the exception that we may have different tools to try and combat it. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour. The most common places where cyberbullying occurs are: Social Media platforms (such as Facebook, Instagram, Snapchat, and Twitter), Text, Instant Messaging, gaming platforms and Email.

What to do if you have concerns

As a user of social networking sites, you may at some time have a concern about what you are seeing or being told about by another user. Concerns may range from negative or abusive comments and cyberbullying to suspected grooming for/or sexual abuse. If you are ever concerned or someone comes to you with concerns you must contact the safeguarding officer, who can then follow it up where appropriate. You must never do nothing.

If cyberbullying occurs

- Never respond or retaliate to cyberbullying incidents.
- You should report incidents appropriately (to both the website/ phone company and safeguarding lead) and seek support and advice from the safeguarding officer.
- Save evidence of the abuse; take screenshots of messages or web pages and record the time and date.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a staff member (youth and children's coordinator, vicar or safeguarding officer) to invite the person to a meeting to address their concerns. The staff member can request that the person removes the offending comments.
    - If the person who posted the content refuses, those involved must attempt to come to a decision on what to do next including who is to report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers, or

support from other agencies, for example, www.saferinternet.org.uk
    - If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or the safeguarding team may consider contacting the local police.
- Online harassment is a crime.

Getting offensive content taken down

- If online content is offensive or inappropriate, and the person or people responsible are known, you need to request they remove it and ensure where possible they understand why the material is unacceptable or offensive.
- Most social networks have reporting mechanisms in place to report content which breaches their terms.
- If the person responsible has not been identified or does not respond to requests to take down the material, the designated lead will use the tools on the social networking site directly to make a report.
    - Some service providers will not accept complaints lodged by a third party.
- In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.
    - Before you contact a service provider, it is important to be clear about where the content is; for example, by taking a screenshot of the material that includes the web address.
- If you are requesting, they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions.
- Where the material is suspected of being illegal you should contact the police directly.

Reporting online abuse

- All staff and volunteers should be familiar with the safeguarding policy which includes procedures for reporting potentially illegal/abusive content or activity, including child sexual abuse images and online grooming.
- In addition to referring concerns to our safeguarding officer, you should immediately report online concerns to the Child Exploitation and Online Protection Centre (CEOP) or the police. Law enforcement agencies and the

service provider may need to take urgent steps to locate the child and/or remove the content from the internet.

- You should report any illegal sexual child abuse images to the Internet Watch Foundation at www.iwf.org.uk
- Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre at https://www.ceop.police.uk
- **Where a child or young person may be in immediate danger, always dial 999 for police assistance.**

Future use

New media

- When choosing to use a social networking site or app other than those already mentioned, you should adhere to the general guidelines as closely.
- Again parental/legal guardians' consent MUST be sought before contacting children and young people via this medium.
- If the site or app becomes a key tool or resource, it should be considered whether this social media policy needs updating to reflect this change.

Computer library/ public access

- Should we decide to set up a group or space that allows or provides children and young people with access to computers, tablets or other devices that connect to the internet we must first create and adhere to a policy that covers the risks and processes that need to be put in place to keep children and young people safe.

Photo and Video Policy:

See separate policy.

For further advice

If you need advice or guidance on any aspect of social media please contact Director of Communications Graeme Pringle at graeme.pringle@covcofe.org or 07507196495

- https://www.nspcc.org.uk/
- https://www.o2.co.uk/help/nspcc/child-protection
- https://learning.nspcc.org.uk/
- https://www.ceop.police.uk/safety-centre/
- https://www.childnet.com/
- https://www.iwf.org.uk/
- https://www.thinkuknow.co.uk/
- https://www.saferinternet.org.uk/
- https://www.getsafeonline.org/
- http://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online
- https://www.connectsafely.org
- https://www.internetmatters.org

Professional reputation further reading

- https://www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation
- https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/professional-reputation
- https://www.saferinternet.org.uk/advice-centre/parents-and-carers/safety-tools-social-networks-and-other-online-services

Cyberbullying further reading

- https://www.stopbullying.gov/cyberbullying/what-is-it/index.html
- http://respectme.org.uk/
- https://www.kidscape.org.uk/
- https://childline.org.uk/
- https://www.ceop.police.uk/safety-centre/
- https://www.iwf.org.uk/
- http://www.saferinternet.org.uk/
- https://www.gov.uk/workplace-bullying-and-harassment
- https://www.connectsafely.org/cyberbullying/

- https://www.onlineschools.org/student-bullying-guide/
- https://www.internetmatters.org/hub/research/new-cyberbullying-guide-for-parents-carers-and-schools/
- https://www.helpguide.org/articles/abuse/bullying-and-cyberbullying.htm/
- Cyberbullying: Advice for headteachers and school staff