## NEW GENERATION CHURCH

## ONLINE SAFETY POLICY, E-SAFETY AND CYBERBULLYING POLICY and ACCEPTABLE USE POLICY.

November 2021

Review November 2022

**When responding to concerns of abuse please refer to our ‘Online Safety Flowchart’.**

 **Online Safety definition:**

*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.

**Policy guidelines for Church Workers/Volunteers**

* Generally maintain good and open relationships with parents and carers regarding communication with them and their children.
* Use an appropriate tone: friendly, but not over-familiar or personal.
* Be warm and friendly, but do not suggest or offer a special relationship.
* Be clear and explicit about information that you need to share; don’t abbreviate or short-cut your communications.
* Be circumspect in your communications with children to avoid any possible misinterpretation of your motives or any behaviour which could be construed as grooming.
* Do not share any personal information with children, or request or respond to any personal information from a child other than that which might be appropriate as part of your role.
* Only give personal contact details to children that are within the public domain of NGC, including your mobile telephone number.
* If children want you to have their mobile phone numbers, e-mail addresses or similar, and communicate with them this way, make sure that their parents know and have agreed.
* Only make contact with children for reasons related to the work of NGC and maintain a log of all electronic contact with individuals or groups including messaging and texting.
* Where possible only use equipment provided by the NGC to communicate with children.
* Respect a child’s right to confidentiality unless abuse/harm is suspected or disclosed.
* Ensure NGC’s domain name or group/logo appears with every Internet post made by a church computer user. Any user may thus be viewed as a representative of NGC while conducting business on the Internet.
* Email should only be used to communicate specific information. (e.g. times and dates of events). It should not be used as a relationship building tool.
* All digital correspondence should be kept and dated.
* When using email/internet for communication with children, it is advised that it should take place between the hours of 9am-5pm (9pm for Free60). Where working with children outside normal office hours, workers should seek advice from their leader but there should be no email communication after 9pm.
* Workers should refrain from using Skype, Whatsapp, or similar forums on a one to one basis as they cannot be recorded. (It can be used for conference calls and is considered appropriate if a project or group uses a web camera, Skype, Zoom or Teams in a group environment for project purposes, and has clear aims and objectives for its use). All such sessions should have 2 adults or be recorded. If in a 1:1 session (in extenuating circumstances, such as a national lockdown) the person should be notifies that they session will be recorded and the recording kept in a secure file.

**Social Media Policy**

* All social media interaction between workers, paid or voluntary, and children under 18 shall be limited to monitored/administrated groups.
* Text and any other media posted shall be subject to the acceptable use policy
* All interaction on social media groups shall be recorded for safeguarding purposes. This includes Whatsapp.
* Any private messages shall be recorded for safeguarding purposes
* Any safeguarding concerns/allegations arising from social media shall be referred onto the safeguarding co-ordinator.
* All users of social media must be above the minimum age limit i.e. 13 for Facebook. In the case of Free60 ages 11-13 can use with written parent/guardian permission.
* Workers should ensure their privacy setting ensure the highest levels of security in order to restrict children being able to see any more than what is relevant to communication within the group
* All social media groups should provide links to statutory authorities such as CEOP, to enable children to report online abuse.

**Consent for photographic images and videos online**

* Photographs that include children will be selected carefully and will endeavour to prevent children from being easily identified.
* Children’s full names will not be used on the website in association with their photographs.
* Permission will be sought before any images are taken or displayed and images will only be used for the specific purpose for which permission was sought for and how the image will be stored if not destroyed. If the intention is to use an image on the internet this must be clearly stated and further permission must be acquired if an image is to be used in a way not originally stated.
* Use of images will reflect 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.

**Cyberbullying and E safety**

 All forms of bullying (including cyberbullying) should be handled as a community issue for the whole organisation. It is important that NGC takes measures to prevent and tackle bullying among children and young people that attend various activities. It is equally important to make it clear that bullying of staff, whether by children, young people, parents or colleagues, is unacceptable.

NGC leaders, youth and children’s workers, parents and children all have rights and responsibilities in relation to cyberbullying and should work together to create an environment free from harassment and bullying.

NGC can offer support to parents on how to help their children engage safely and responsibly with social media, perhaps through a parents’ evening, advice in a newsletter or signposting to other sources of support and advice.

It is not acceptable for young people, parents or colleagues to denigrate and bully staff via social media in the same way that it is unacceptable to do so face to face.

All staff are in a position of trust, and there are expectations that they will act in a professional manner at all times. Here is some key advice for staff which may help protect their online reputation:

* Enabling a PIN or pass code is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by anyone.
* Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
* Consider your own conduct online; certain behaviour could breach your employment code of conduct.
* Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
* Do not accept friend requests from children or young people who attend or have attended activities arranged by NGC. If you feel this is necessary, you should first seek guidance from someone on the leadership team. Be aware that your social media friends may also be friends of parents or family members, of children or young people in your care and therefore could read your post if you do not have appropriate privacy settings. It is recommended that you have all privacy setting set to the highest level and that you do not engage in Private/Discreet messages with any young/unknown person.
* Do not give out personal contact details – if children or young people need to contact you with regard to activity arrangements, always use NGC ‘s contact details. When using Whatsapp to contact young people the leader must have parent/gradian permission. Always use Email in the first instance until parent permission in gained, then group message. There must be at least 2 team members included in any group or direct messaging that is conducted.
* Use NGC’s email address for business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

**If you are bullied online**

* You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your team leader or the leadership team of NGC.
* Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
* Where the perpetrator is known to be a child or young person, the majority of cases can be dealt with most effectively through talking with the perpetrator and offering them help and advice.
* Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a leader to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
* If they refuse, it should be the leadership’s decision what to do next – either 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, The UK Safer Internet Centre.
* If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you may consider contacting the local police. Online harassment is a crime.

Employers have a duty to support staff and no-one should feel victimised in the workplace.

The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

All employers, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by young people, parents and other members of staff and supporting them if it happens.

For more information on protecting children and young people from cyberbullying see

 **InFocus: Cyberbullying - Keep Children Safe Using ICT**

**Nb: The use of the term staff includes all people both payed and volunteer wo are acting on the behalf of the church.**

**Acceptable Use Policy (To be included with consent/registration forms for children and young people with a request for acknowledgement by both parent and child)**

* Where access to the internet is provided on devices owned by an individual via WiFi, we will exercise our right to monitor usage which includes access to websites, interception and deletion of inappropriate or criminal material or unlawfully copied text, video, images or sound.
* WiFi Access will be via a secure password that will be changed quarterly.
* Social media groups must be used in compliance with NGC’s policy on social media.

**Children and Workers should not:**

* Search for or download pornographic, racist or hate motivated content.
* Illegally copy or play copyrighted content where permission has not been given.
* Send, request or display offensive messages or pictures.
* Harass, insult or bully others.
* Access the internet using another person’s login details.
* Access, download, send or receive any data (including images), which NGC considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
* Access another person’s phone.

**Sanctions for violating the acceptable use policy in the opinion of NGC** **may result in:**

* A temporary or permanent ban on internet use.
* Additional disciplinary action in line with existing practice on inappropriate language or behaviour.
* Where applicable, police or local authorities may be involved.

**Parent Carer Agreement**

As the parent/guardian of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ I declare that I have read and understood the Online Safety acceptable use policy for New Generation Church and that my child will be held accountable for their own actions. I understand that it is my responsibility to set standards for my child when selecting, sharing and exploring online information and media.

**Child/YP Agreement**

I understand the importance of safety online and the church guidelines on acceptable use.

I will share any concerns, where I or another person may be at risk of harm with the safeguarding coordinator or a trusted adult.

|  |  |  |
| --- | --- | --- |
| **Child Name** (Please print) | **Child Signature** | **Date** |
|  |  |  |
| **Parent/Guardian** (Please print) | **Parent/Guardian Signature** | **Date** |
|  |  |  |