ONLINE SAFETY POLICY

Who is this policy for?
All CityGates Church Norwich Employees and Volunteers including permanent staff, contract staff, temporary staff or others who may be working for CityGates Church for a defined period of time.

1. Introduction

The purpose of this policy is to:

- Ensure the safety and wellbeing of children and young people when adults, young people or children are using the internet, social media or mobile devices and interacting with CityGates online profile;
- Provide staff and volunteers with the overarching principles that guide our approach to online safety;
- Provide clarity to all those within the church about how to conduct online communications, both when representing the church, with children and adults.

Social media in particular brings many opportunities, especially for evangelism, and so we want to make sure we use it safely.

2. Definitions

2.1 'Online safety' is the collective term for the practice of using the internet and the protection from the risks of being online including the use of electronic devices and applications to communicate and access the internet.

2.2 'Social Media' includes any websites and applications that enable users to create and share content or to participate in social networking. Some of these include Instagram, Snapchat, Facebook, YouTube and Twitter. More general forms of online communication could be emailing, messaging and online videoing (e.g. Facetime or Zoom).

3. General guidelines for staff and volunteers

As those who work or volunteer within the church, our lives are to be an example to those who know us. Therefore, our online lives and presence must reflect who we are in Christ and these are just as important as how we act face-to-face. Similarly, our online lives shouldn't misrepresent or exaggerate who we are in reality.

General guidelines:

- As representatives of CityGates Church and the gospel we shouldn't use social media and online communication to encourage people to do anything that the Bible would disagree with
- Do not post or message negatively about CityGates Church, use defamatory language or breach copyright when posting images, videos or links
- While online communication and social media usage are valuable tools for many areas, these shouldn't replace time spent with people in person
- When using online communication, use an appropriate tone: friendly, but not over-familiar or personal. Be very clear to avoid any possible misinterpretation
- With specific reference to young people, all communication between church workers/volunteers and those under the age of 18 must be in accordance with the youth 1-2-1/pods policy, including all online communications to take place through group chats with a parent electronically present
- It is your responsibility to ensure your computer and accounts are properly protected while online and use the correct privacy setting to restrict access
- Always consider confidentiality and personal information; do not share anything that isn't yours/you don't have permission for.

4. Our responsibility

4.1 We reserve the right to block any social media account from accessing CityGates Church accounts, if it is deemed appropriate to do so.

4.2 We will take reasonable steps to ensure our social media accounts are secure from unauthorised users. CityGates Church social media accounts will only be used and accessed by CityGates Church staff, as defined at the top of this policy.

4.3 Members of the Operations Team and CGCN Trustees have the right to check what is happening on any CityGates Church social media account and ask the named users about these.

4.4 We reserve the right to protect our accounts by monitoring posts and messages and reacting appropriately.

4.5 We reserve the right to remove access rights from any individual or group who might be violating this policy.

4.6 Any pictures or videos posted should (as much as is possible) contain the 'Young CityGates' and/or 'CityGates' logos to show that the post is supported by the church. All social media accounts' profile pictures are of these logos additionally, which will further show where it is coming from.

5. Messaging services ie WhatsApp

5.1 Consent must be gained before adding people (of any age) to Whatsapp groups as their number will appear for others to see. Members will always have the ability to leave an online group personally.

6. Video software ie Zoom

6.1 When needed CityGates Church staff and volunteers use video software to conduct online meetings.

6.2 Ideally the software to be used should be the CityGates account for Zoom. When using this account, every meeting should be set up to include a meeting ID and password, which should only be communicated to those taking part. Zooms should also always make use of the 'waiting room' option so that the host can see who is trying to enter the meeting and give permission to do so.

7. Safeguarding

7.1 Any safeguarding issues that arise through online communication and/or social media should follow the procedure of the CityGates Church safeguarding

policy and should additionally be reported to the CityGates Church safeguarding lead.

7.2 Any concerns or issues online shouldn't be followed up or investigated further using social media by workers or volunteers. Rather, concerns should be passed on to the Safeguarding Lead.

7.3 Staff should not follow any under 18s involved in any youth work at CityGates Church on Instagram or follow them on Facebook.

8. Photographic images and videos online

8.1 If photos are going to be taken at an event or during a Sunday service, all individuals should be made aware, either via signage or an announcement.

8.2 Use of images and videos should reflect diversity of age, ethnicity and gender as much as possible.

9. Record Keeping

9.1 All interaction on any social media sites either between adults or between an adult and a young person should be retained, not deleted, so these can be referred to whenever needed, especially private messaging.

10. Young People

10.1 General Guidelines

The use of phones when meeting with young people in person should be very limited. Volunteers and church staff should not use their phones in the presence of young people and children if possible.

If phones must be used, e.g. for photograph taking, a designated phone should be used (usually the leaders) or a designated camera.

Where possible, encourage young people to not be on their phones when meeting unless in severe cases, particularly for neurodiversity where a plan should be made with the parents/carer. There is not a need to collect these from the young people, but use of phones should be discouraged.

10.2 Messaging Services ie WhatsApp

When messaging young people, e.g. via WhatsApp, iMessage or text make sure that parents have given permission for the communication beforehand.

10.3 Safeguarding

For children and young people involved in any youth work at CCGCN, consent forms are to be completed to comply with safeguarding regulations. These consent forms contain a section of asking for permission from parents/carers about taking photos of young people and using these on CGCN social media accounts.

To make sure forms are in line with parental preferences, these will be updated annually by all parents/carers and photos used on social media will reflect this.

10.4 Photographic images and videos online

Names and details will never be given out or shown when photos/videos are published.

10.5 Times of communication

Staff and volunteers at CGCN should try to restrict communication online or via social media to within the hours of 9am and 9pm. This is to stop young people from becoming reliant on the conversation and encourage them to be off social media.

Exceptions to this may happen if organising a trip, such as the Sorted Conference, needing last-minute information or in emergency situations.