DIOCESE OF CANTERBURY
eSAFETY GUIDELINES

The internet and the online world is constantly changing but fixed as an integrated part of our contemporary lives. A fundamental shift among internet users is the change from 'consumer' to 'contributor' - the internet is now wholly interactive. Younger generations are growing up in a world where contributing to the media is a natural part of life. Older generations can find the public nature of Social Media disconcerting and may see it as potentially dangerous.

Against this backdrop, we need to consider how to use Social Media safely and effectively. The overarching principle is to find mechanisms and protocols to help us use our best safeguarding practise for physical groups and interactions in this online space. Encountering a new form of online interaction, it is important to compare it to a similar interaction in the physical world. Using this approach, we can find the best tension between risk and trust, as we seek to safeguard children, young people - and ourselves.

Throughout this document when we refer to a 'leader', we mean someone safely recruited (including references and DBS) and a current member of a ministry team.

A 'supervisor' is the appropriate person any 'leader' is accountable to.

General points when communicating especially with a younger person via technology:

- Do not delete anything that is sent – either from you, or to you
- There is an advisable curfew on communicating after 11pm
- Church leadership could ask to check messages at any time. This encourages accountability and reduces the potential for concerns to be raised in respect to secretive activity.

GRiD PLAN

GOOD — RISK — DON'T

GOOD: *What is the benefit and potential?*
RISKS: *What are the relative risks involved?*
DON'T: *What practises and habits are best avoided?*

The **GRiD** plan uses three sections to explore using the internet to support the relationships and communities that churches are seeking to build.

'GOOD' identifies benefits, including some ideas worth considering.

'RISKS' outlines the relative dangers involved - our intuition is often wrong in evaluating relative risk: planes *feel* more dangerous than cars but the real risk of injury is far higher on the road *than in the air. Risks must be reasonably evaluated and considered within the appropriate* context.

'DON'T' simply best avoided when using Social Media and other online tools.

1. EMAIL

GOOD
- quick, cost effective and paperless communication.
- easy to send newsletters, information and adverts to a securely held list of email addresses without the need for a database. Yahoo and Google operate free distribution lists called 'Groups' and online distribution tools like [Mailchimp](http://www.mailchimp.com)[1] are also widely used.

RISKS
- when communicating with children and young people, individuals and their parent/guardian consent should be obtained. This is done most simply when an individual registers to join a church group.
- a ChYP's Ministry Leader should use a specific and known account to communicate with the children and young people. The address should be known to the young people, children, parents and the leader's supervisor. The leader's supervisor should be able to access all messages, both sent and received on this account. Under no circumstances should messages be sent or received on a separate account. Children, young people and parents should be aware that the supervisor has access to the account, simply done at the time consent is given.

DON'T
- use flirtation, crude humour, ridicule or insulting language, even in jest. Clear and unambiguous language should be used as nuance and tone in email can often be hard to read.
- use abbreviations that can be misinterpreted, such as 'lol' ('laugh out loud' or 'lots of love').
- say anything in an email you would not say face to face.

---

[1] http://www.mailchimp.com

2.   PHOTO-SHARING

Photo-sharing sites such as Flickr/Instagram provide opportunity to store, sort, search and share photographs online. Some photo-sharing sites are themselves a form of Social Media.

GOOD

- Photos of events or group activities are accessible for the whole community
- Taking pictures in the moment can greatly increase the effectiveness of sharing stories or advertising events.

RISKS

- Always take care to ensure consent is obtained before taking any photographs or making them public.
  Please Note: The Diocesan Policy and Guidelines for photographs applies in all contexts!
- An image (or text) taken out of context may give a very misleading impression. Ask yourself what impression an image will give to someone seeing it out of context.

DON'T

- take offensive, inappropriate or illegal images.
- upload images of anyone without their express consent.
- assume that something you think is funny will be considered so by everyone else.

3.   VIDEO-SHARING

Video-sharing sites, such as YouTube*, similar to Photo-sharing, allow users the to upload, view and share videos. They display a wide variety of user-generated video content, including movie clips, TV clips, and music videos, as well as amateur content such as video blogging and short original videos.*

GOOD

- Film and video is an art-form that may engage a wide section of a church community. Consider how you might use YouTube to broadcast short video messages from a group, or about a subject.
- Recording talks, sermons or drama makes them accessible to the whole church community, including those who are not always physically present.
- Video is extremely effective in advertising events or regular groups.

RISKS

- remember the need for consent.
- Video (and audio) is relatively easy to edit. There is a risk of being misquoted or a comment to be used out of context.

DON'T

- upload any video featuring someone without their consent.
- upload any portion of video that is subject to copyright.
- forget that the internet is in the public domain!

SOCIAL MEDIA

Social Media is a form of communication across web-based software and mobile technologies. The biggest criticism of Social Media is the matter of security and data protection - it is therefore important to remember that the User is in control. However, we must ensure that we accept and allow for varying perspectives and opinions about privacy.

All Social Media platforms are very careful to ensure that the user has full control of the security and privacy settings of their profile (including comments, picture, personal information etc.) There will always be a default security setting, but as with all computer and internet usage, it is the user's responsibility to customise their settings.

1.   FACEBOOK

Founded in 2004, Facebook's mission is to make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them. [fb newsroom][2] *Users must register before using the site, after which they may create a personal profile, add other users as [friends][3], and exchange messages, including automatic notifications when they update their profile. Additionally, users may join common-interest user groups, or 'Like' organisation's Facebook Pages.* [wiki][4]

GOOD

- Facebook is an excellent way to develop the community of a church or group. It provides a more constant source of connection for those on the edge of the community, or those who struggle to be physically present.
- Facebook has two mechanisms to help organisations connect and interact with users: a 'Facebook Group' or a 'Facebook Page'. A Facebook Group: a community of people and friends promote, share and discuss relevant topics. Groups, Pages and Events (below) are created by a Facebook user, who automatically becomes the 'Admin'. They then have control of the settings of the group, page or event. The 'creator' can assign 'Admin' status to other members of the group, page or event, and designate how much control each then has.
- Events can also be created in Facebook, allowing users to advertise events. Anyone invited will become members of the event and can RSVP, share photos before or after the event, comment and engage in discussions.
- Sharing photos, links, videos and engaging in forum discussions all provide additional opportunities for churches and youth groups to develop discipleship outside of the Sunday Service.
- Facebook provides a unique opportunity to build relationships with young people's parents, when parental consent is sought for interactions with young people. Parents could also be invited to join the Group or to 'Like' the Page.

RISKS

- Control lies ultimately with the user. All Facebook users need to be encouraged to customise their security settings. [i.e. the extent of personal information shared and with whom],
- Leaders should be assigned 'Admin status' on all Groups and Pages and monitor comments, the wall, images and the behaviour of members of the Group or Page. Leaders should feel free to challenge or intervene as necessary. If a Facebook Group or Page is set up in the name of the

---

[2] http://newsroom.fb.com/content/default.aspx?NewsAreaId=22
[3] http://en.wikipedia.org/wiki/Friending
[4] http://en.wikipedia.org/wiki/Facebook

church or youth group, it is essential that a leader becomes a member of it and oversees the content and activity.

- Facebook Protocols need to be agreed within any Youth Ministry Team (including leaders and workers, whether employed or voluntary).

- Similarly, Young People should be openly encouraged to be conscious of their activity on Facebook; including the information and photos which may be shared, and times appropriate for members of the Facebook Page/Group to communicate with each other.

- There is a risk in any adult being 'friends' with a young person on Facebook. However, this is often the most effective way of communicating with young people. A leader may accept a friend request from a young person on Facebook, but should set their personal privacy settings appropriately**.** No private messages should be sent to young people from either individual leaders they are 'friends' with, or to a leader as a 'group' Admin representative. If a young person contacts a leader via a private message, the leader should tell their Supervisor immediately. They should then reply, explaining they need to invite another adult to the conversation/suggest to email and include another adult/suggest to talk in the regular group setting.

- When a leader stops their involvement with their ministry they commit to a conversation with the Ministry Team Leader re friendship status with young people on Facebook. Please refer to the Volunteer Agreement signed in the safe recruitment process for further details.

DON'T

- set up a separate Facebook profile. Although encouraged in some sectors, this practise is in direct contradiction to Facebook's Terms & Conditions. Any one person is only allowed to manage one Facebook account. See above for notes on creating a Facebook Page or Facebook Group.

- delete any messages sent to a young person in case of future allegations.

- say anything on Facebook you wouldn't say in public or want repeated.

- encourage anyone under the age of thirteen (13 years old) to register on Facebook. The safeguarding policy and practice should include agreed protocols, such as minimum age of users, which should be set at or above the minimum required by Facebook terms and conditions.

2.   TWITTER

At the heart of Twitter are small bursts of information called [Tweets](#)[5]. Each Tweet is 140 characters long, but don't let the small size fool you—you can discover a lot in a little space. You can see photos, videos and conversations directly in Tweets to get the whole story at a glance, and all in one place. [twitter.com](#) [6] Twitter is the most public of all Social Media communications. Although it is possible to send a Direct Message [DM] to another Twitter user, all general Tweets are public. This openness is Twitter's greatest advantage as long as all users remember it.

GOOD

- Twitter users tend to be students and young professionals, whereas Facebook has a far broader mix across all age groups.

- Unlike Facebook, multiple accounts per user are allowed. As such, many people have both a corporate and personal Twitter account.

---

[5] http://support.twitter.com/articles/15367-how-to-post-a-twitter-update-or-tweet
[6] http://www.twitter.com/about

- Hashtags (#tags) are very useful in filtering comments and interactions and provide a mechanism for conversations on Twitter.
- Integration between Twitter, Facebook and Blogs means that Social Media is a very powerful mechanism for churches and youth groups.

RISKS

- All Twitter users need to be conscious that it is, by its very nature, a public forum. Used appropriately this has immense benefits, but it is easy to forget 'where you are'.
- One of Twitter's selling points is that a user may be 'followed' by anyone, anywhere. If this is not appropriate or desirable, the account can be hidden from public searches.

DON'T

+ say anything on Twitter that you wouldn't say live on the radio.
  NB: Remember all Tweets are public.

MOBILE COMMUNICATION

Mobile devices have become handheld computers. Users can create presentations, word documents and send emails all whilst walking to work. Users can connect to their chosen Social Media on the move, while retaining the standard mobile functions of text, voice and even video calls.

GOOD

- Mobile communication offers users the ability to contact or be contacted when away from the office environment. Given that ministers are often on the road, between clubs, schools and meeting people, mobile phones can increase availability.

RISKS

- Being constantly available risks the work-life balance. If mobile communication (including Social Media) is used in ministry, it is up to the leader to ensure appropriate boundaries. It takes self-discipline to disengage from emails, texts, Facebook and Twitter, but it is incredibly important to safeguard free-time.
- A record of conversations needs to be kept, as with all forms of digital communication
- It is important to check the security settings of any mobile devices. The manufacturers default settings may be sufficient, but it is the users' responsibility to customise their own devices.

DON'T

- send inappropriate texts or images.
- allow anyone else access to the mobile device. It is important to safeguard the contact information that will be within the mobile device.
- allow the mobile device to control your work patterns: you are allowed to turn it off!
- use your mobile phone when driving!

YOUNG PEOPLE ONLINE

1.   CYBER BULLYING

Cyber Bullying is very common and can happen to a child of any age. There is even the potential for 24 hour bullying, which is very distressing. Once bullying might stop once the young person left school. Today, with the advancement of technology, bullying may follow the young people home through their mobile telephones, emails and Social Networking Sites. Beatbullying is an online website working at the forefront of cyber bullying and offers online mentoring from other young people who have been trained by Beatbullying. It is essentially a safe Social Networking Site. Free counselling is also available. www.beatbullying.org [7]

The practice of cyber-bullying is not limited to children. It is often referred to as cyberstalking or cyberharassment when perpetrated by adults.

If you have concerns about the conduct of someone you know, you should contact a member of the Diocesan Safeguarding Team.

The best defence for the potential anonymity offered by the internet is education. There is always a risk of interacting with someone who claims to be a different age or gender, but this needs to be weighed up against the overall benefit of online communication. Any children or young people who have access to the internet need to be made aware of the risks and given some basic advice and oversight to keep them safe.

- Never give out personal information to online friends. This includes an instant messaging ID, email address, mobile number, school name and any pictures of you, your family and friends.
- Remember online friends are just that. If they are unknown to you in the real world, they may be lying about who they are.
- Children and young people should never meet with a person they have met online, unless they take a trusted adult with them.
- If something is published online, anyone can access it, change it or share it with others. Keep social network profiles private.
- Use webcams with caution and only with family and friends who are already known in the real world. Images can be copied, changed and shared.
- Do not post inappropriate images of yourself online, which send out the wrong impression and make you vulnerable.
- Think before opening files from people you do not know in the real world. They may contain anything from a virus to an inappropriate image or film. They should be deleted.
- Know how to block someone online and report them to the Child Exploitation and Online Protection Centre (CEOP) if you feel uncomfortable. Save the http://www.clickceop.net website to your favourites, so that you can report any suspicious behaviour straight away.

1.   BLOGS

*A **blog** (a portmanteau of the term **web log**) is a personal journal, published online, consisting of discrete entries ("posts") typically displayed in reverse chronological order. so the most recent post appears first. Blogs are usually the work of a single individual, occasionally of a small group, and often are themed on a single subject. Most good quality blogs are interactive, allowing visitors to leave comments, and even message each other, on the blogs. It is this interactivity that distinguishes them from other static websites.*wiki [8]

---

[7] http://www.beatbullying.org/
[8] http://en.wikipedia.org/wiki/Blog

GOOD

- Simplest and cheapest form of website
- Allows for automatically archived and categorised content. This makes blogs ideal for sharing sermons, small group notes, reports on events, immediate response to relevant news and more.
- Enables comments on posts, providing an online discussion forum for the Church Community, as well as a pace to gather feedback.
- Posts can be used to gather a library of resources or articles from around the World Wide Web.

RISKS

- Anything posted on a blog is immediately within the public domain – there is no way to un-say something. Always take care: if you wouldn't say it to a crowded room, don't say it on a blog post.
- Enabling comments on posts is generally open to anyone. There is a risk of abusive or offensive language being used by those unknown to you or your community. Such comments are easily removed by the blog's author. To avoid this risk, comments can be disabled (which removes the advantage of discussion) OR comments can be made subject to approval by the blog author. In this case, the author or administrator of the blog will be notified that a comment is awaiting approval. The risk of abusive comments is most likely outweighed by the advantage of an open forum, especially if inappropriate comments are quickly removed.

DON'T

- Use inappropriate, offensive or illegal content. Including pictures, video, text and audio.
- Plagiarise. Most bloggers are happy to have their content reposted on another blog, but they do expect to be credited and for readers to be able to click through to the original site. A link-back is easily inserted into the post referencing from where the content been copied.
- Please ask the author's permission first!
- Forget that blogs are in the public domain.

CHANGING ONLINE WORLD

Given the nature of social media and the whole realm of online interactions, this document needs to be updated more regularly than other guidelines. If you have any experience of dealing with Social Media which would add to the scope of effectiveness of these guidelines, please let us know. Please send a digital copy of any adapted or summarised parish guidelines to the ChYP's Ministry Team for information.

USEFUL LINKS

http://www.youtube.com/ceop
http://www.childnet-int.org
http://ceop.gov.uk
http://thinkuknow.co.uk
http://ccpas.co.uk
http://www.beatbullying.org
http://www.cybermentors.org.uk