CYBER SAFETY

Guide to Cyber Safety

The Baptist Union of Great Britain

Contents

1. WHAT IS CYBER ABUSE?

Cyber abuse is the use of information technology (email, mobile phones, websites, social media, instant messaging, chatrooms, etc.) to harm or harass other people in a deliberate manner. It can include communications that seek to intimidate, control, manipulate, put down, falsely discredit, or humiliate the recipient. It may also include threatening a person's earnings, employment, reputation or safety.

Cyber abuse is also referred to as Cyber Bullying and Cyber Stalking, and with the increase in use of computer technologies, it has become increasingly common.

Unlike other forms of abuse, cyber abuse can happen at any time and is not limited to a specific location. A person can experience cyber abuse even when they are alone. This means that those on the receiving end of cyber abuse have a harder time getting away from the abuse.

In addition, cyber abuse messages and images can be posted anonymously and distributed quickly to a wide audience. It is extremely difficult to completely delete inappropriate or harassing messages, texts, and pictures after they have been posted or sent, and there is little or no control over what people do with them once received or seen. It is also not always possible to trace the source of the abusive material.

There are a number of characteristics which can define cyber abuse:

- ***Anonymity***

  Cyber abusers often use the internet using pseudonyms
- ***Accessibility***

  Cyber abusers can approach their target at any time
- ***Bystanders***

  Bystanders to abuse in the cyber world can be numerous
- ***Loss of inhibition***

  The anonymity of the internet can encourage an individual to commit acts they might not otherwise attempt in person. They feel a greater sense of bravado when they think they cannot be identified.

2. WHO PERPERTRATES CYBER ABUSE?

A cyberbully may be someone known to the person being abused, or they may be an online stranger. They may be anonymous and may solicit involvement of other people online who do not even know the target. Due to this anonymity, most people think that bullying or abusing online is easier to get away with than bullying or abusing in person.

Research in the USA suggests that females are about twice as likely as males to be victims and perpetrators of cyber abuse.

3. FORMS OF CYBER ABUSE

There are a number of different forms of cyber abuse, including:

- ***Harassment*** - repeatedly sending offensive, rude and insulting messages
- ***Denigration*** - posting derogatory information about someone, and/or digitally altered photographs
- ***Flaming*** - fighting online, often using vulgar language
- ***Impersonation*** - hacking another's email or social media account to post embarrassing material
- ***Outing and Trickery*** - sharing another's secrets or tricking someone into revealing embarrassing information
- ***Cyber Stalking*** - repeated threats or online activity that makes a person afraid for their safety
- ***Trolling*** - the starting of arguments in online communities and online insults, provocations and threats
- ***Grooming*** - building an emotional connection with a person in order to gain their trust for the purposes of sexual abuse or exploitation
- ***Sexting*** – sharing inappropriate or explicit messages online or via mobile phones

It is worth noting that cyber abuse is not just a teenage problem. Many younger children and vulnerable adults have also been targeted for this type of abuse.

4. INDICATORS OF CYBER ABUSE

Without having access to their mobile, tablet or computer, it can be difficult to know if someone is experiencing cyber abuse. Some indicators of this form of abuse may include:

- Low self-esteem
- Withdrawal from family and spending a lot of time alone
- Reluctance to let parents / carers or family members anywhere near their mobile, tablet, laptop, etc.
- Friends dropping away
- Being excluded from social events
- Finding excuses to stay away from school or work
- Changing appearance to try and fit in
- A change in personality i.e. anger, depression, crying, becoming withdrawn, etc.

Cyber abuse can affect anyone at any age and may leave someone feeling very upset and alone.

It may be a constant source of distress and worry, as there is no escape from the abuse which may be occurring at school or work, continuing at home or when out and about, day after day.

5. RESPONDING TO CYBER ABUSE

It can be very easy to post malicious and hurtful posts on social media sites, with little moderation, and posts can go "live" before they can be reported. This may leave people feeling extremely vulnerable and at a loss as to what they can do about it. However, people do not need to suffer in silence, as there are things that can be done to help address this issue.

Advice for those being abused on the internet:

- **Do not respond** to and don't forward abusive messages or posts - emotional reactions are what is wanted, so don't give them the satisfaction
- **Block the person** who is cyber bullying – although this doesn't stop it from continuing, it will save you from having to see the abuse
- **Send a short warning** message, such as "*do not contact me again*", and record this along with any further contact with the person
- **Keep evidence** of cyber abuse - record the dates, times and descriptions of instances when cyber abuse has occurred. This can be done by saving and printing screenshots, emails and text messages
- **Report** anyone who starts to become abusive - most sites have strict rules about bullying behaviour and will have a "report abuse" button. You can also report abuse to mobile phone providers if it is taking place via text messaging
- **Report** the abuse to your school / workplace if you suspect a fellow student / colleague is being abusive
- **Report** the abuse to the police if the abuse includes
    - Threats of violence
    - Child pornography or sending sexually explicit messages or photos
    - Taking a photo or video of someone in a place where he or she would expect privacy
    - Stalking, trolling and hate crimes
- **Find someone to talk to** about what is happening – this could be someone you know or someone who understands cyber abuse (*see section 7 for key contacts*)

If you have any questions, or need more information and support when dealing with cyber abuse, please contact your local Association Safeguarding Contact (*details of which can be found in the safeguarding section of the BUGB website)*.

6. GOOD PRACTICE GUIDELINES FOR CYBER SAFETY

Passwords

Keep your passwords safe and do not share them with others, as this can compromise your control over your online identity and activity. If someone discovers your password, change it as soon as possible. Try to pick an unusual password and use letters and numbers within it. Do not use things that are easy to guess, such as any part of your name, email address or your birth date.

On-site protection

Always make sure that the sites you use have clear abuse and harassment reporting facilities.

Check settings

Check the current settings on any social media accounts and consider who you would want to see information or pictures that you post online. Should complete strangers see it? Friends only? Friends of friends? Change the settings if necessary.

Please Note: we recommend that you check these settings regularly, as social media sites frequently update their privacy settings.

Search Engine Check

If you are not sure about someone, online search their user or profile name to see if there are any negative comments about them, or if they have a history of trolling or abuse. It is also a good idea to search your own name online from time to time, to double-check what personal information you or others have made public.

Advice for Parents / Carers

Try to be aware of what your children are doing online, including the sites they visit and who they are interacting with. Installing parental control filtering software or monitoring programmes may be helpful for monitoring your children's online behaviour, but do not rely solely on these tools.

Make time to regularly talk with children about cyber abuse and other online issues, including helping them to consider what they post or say about themselves or others. Children and young people are not always aware that once something is posted, it is out of their control as to whether someone else will forward it.

Church Computers / Wi-fi Usage

If your church has computers which others may have access to, make sure that there are suitable parental controls and blocks put on. Although this is not failsafe, it will make it more difficult to use the computers for inappropriate behaviour, whilst also protecting any children, young people or adults at risk who could be using them.

You may want to create a policy specifically for church computer and wi-fi usage, including terms and conditions for use, as well as what will happen if someone breaches these conditions, such as using a church computer or wi-fi connection to send abusive cyber messages.

A range of sample policies can be found online, such as from the UK Safer Internet Centre: *www.saferinternet.org.uk*

Pictures

With mobile phones and tablets with cameras, it is easy to take pictures and immediately upload them to the internet. Make sure that you have an individual's clear permission to take a picture and that they're happy for people to see it online.

Don't let anyone take pictures of you that you don't mind other people seeing. This is particularly important for children, young people and adults at risk. A good rule for children is *"would you want a parent / carer to see them?"* If not, don't let anyone take them or make you take them.

Think before you type

Nothing is secret in cyber space and something that you write or post now may impact your life later, for example, future job prospects. Employers may search the internet before they hire you, and so may new friends, colleagues or potential partners.

7. KEY CONTACTS

There are a number of organisations who specialise in cyber abuse and supporting and helping those experiencing it. For further information and specialist advice, please contact:

CEOP Command

The National Crime Agency's CEOP Command (formerly the Child Exploitation and Online Protection Centre) identifies the main threats to children and coordinates activity against these threats to bring offenders to account. CEOP protects children from harm online and offline, directly through National Crime Agency led operations and in partnership with local and international agencies.

To report suspicious behaviour online with or towards a child, click the CEOP button found throughout the internet, or use the CEOP online reporting form which can be found on their website: www.ceop.police.uk/safety-centre

If you think a child is at immediate risk, call 999.

To report illegal content online, contact the Internet Watch Foundation: www.iwf.org.uk

To report a crime anonymously, contact Crimestoppers on 0800 555 111

Think U Know

Resources and all of the latest information about new technologies and sites children and young people are visiting.

www.thinkuknow.co.uk

Bullying UK

Bullying UK is part of Family Lives, a charity supporting and helping parents with issues that are a part of family life.

www.bullying.co.uk/cyberbullying

0808 800 2222

The Cybersmile Foundation

A non-profit organisation trying to combat cyber abuse, which has been set up by parents of children directly affected by cyber abuse.

www.cybersmile.org

This guide has been produced for use in Baptist churches in England and Wales.

Guide issue date: 22 December 2015