LONDON DISTRICT OF THE METHODIST CHURCH

Safeguarding: Working Online Safely

Guidance for communicating & working safely with people online

Section 1

1.0 Guidance Review

Last Review Date	Type of Review	Next Review Date
April 2020 (created)	Full Policy	April 2021
May 2020 (edited)	Addition – PREVENT	April 2021
May 2021 (edited)	General review	April 2022
December 2021 (edited)	General Review	April 2022

1.0.1 Context of Changes

In this edition, text in ***bold, italic and highlighted grey*** differs from that of the previous edition and ***[…]*** indicates a deletion.

1.0.2 Table of Amendments

Page No.	Section	Update
4	2.0	About this guidance – links updated
13	4.0.11	Record Keeping / Monitoring – link updated
19-20	7.0	Additional Sources of Support

Contents

SECTION 1 1

1.0 Policy Review 1
1.0.1 Context of Changes 1
1.0.2 Table of Amendments 1

SECTION 2 4

2.0 About this Guidance 4

2.1 Purpose 5

SECTION 3 5

3.0 What Are the Risks? 5

SECTION 4 6

4.0 Good Practice Guidelines 6
4.0.1 Code of Conduct 6
4.0.2 Acceptable Use / Online Safety Agreement 7
4.0.3 Online Safety Policy 8
4.0.4 Profiles and Personal Accounts 8
4.0.5 Devices and Passwords 9
4.0.6 Call Set-Up & Admin 10
4.0.7 Children & Parental Consent 10
4.0.8 When a parent or carer is not willing to give consent for an activity 11
4.0.9 Group Calls / Video Meetings / Online Activities / Messaging 11
4.0.10 Livestreaming 12
4.0.11 Record Keeping / Monitoring 13
4.0.12 Domestic Abuse 14
4.0.13 Prevent 14

SECTION 5 16

5.0 Reporting Concerns 16

SECTION 6 17

6.0 Definitions 17
6.0.1 Online Safety 17
6.0.2 What is classed as 'inappropriate'? 18
6.0.3 Inappropriate 18
6.0.4 Illegal 18

6.0.5 Prevent.....19

SECTION 7.....**19**

7.0 Additional Sources of Support:.....**19**

Section 2

2.0 About this Guidance

This guidance has been formulated as a result of the Government's instruction on social distancing due to Coronavirus (COVID-19) concerns and the requirement for remote working using online platforms and telecommunication.

The Methodist Church has to be creative in how we connect with our congregations, each other and those we support. One of these innovative ways is to use digital technologies. However easy and straightforward some of us may find this; it is not without its pitfalls.

This guidance will be periodically reviewed and updated to identify any 'gaps', address poor practices or challenges to safe engagement.

When reading this document, it should be assumed that the term:

- 'Worker' encompasses both paid and voluntary staff as well as Ministers and lay employees
- 'Participant' encompasses everyone we may engage with using online and digital media

The guidance should be read alongside:

- ***Social Media Guidelines HERE.***
- ***Creating safe and engaging virtual spaces with children and young people HERE.***
- ***Using social media for churches: HERE.***

As well as the following policies and guidance found HERE:

- ***Safeguarding Policy, Procedures and Guidance for the Methodist Church in Britain***
- ***Domestic Abuse Policy and Procedures***
- ***Safer Recruitment Policy***
- ***Practice Guidance on Carrying Out DBS Checks as part of Safer Recruitment***

2.1 Purpose

The purpose of this document is to provide guidance on how to navigate this digital form of communication, while still safeguarding children, young people and vulnerable adults.

Online work can take many forms, but these might typically include:

- Meeting as a group or with individuals through an online video chat platform, such as Microsoft Teams or Zoom.
- Connecting with individuals and groups through messaging software, WhatsApp being highly popular.
- Broadcasting or going 'live' to share sermons, activities or video's on social media platforms, such as Facebook or YouTube.

Each of these provide a great opportunity to connect with people during this period of isolation, which otherwise might not happen. However, this all comes with its own set of risks, which we need to understand and plan for.

Section 3

3.0 What Are the Risks?

It is important to remember that communicating with an individual one to one online, whether via messaging or video, is the equivalent of meeting that person in a room on your own with no one else around.

Communicating with groups and holding virtual gatherings using online platforms also presents challenges to consider.

In addition, some people do not have access to reliable technology or to technology at all, so when planning activities that are only accessible online, we should consider who might inadvertently be left out or isolated. Consider whether anyone has additional needs that might prevent him or her from fully taking part. Does the time of the meeting align with the rhythms of the people you work with?

The following list is not exhaustive, but highlights some risks to keep in mind:

- Opportunity for grooming/sexual exploitation
- Inappropriate conversations between participants and workers
- Potential allegations against workers

- Sharing of worker or participant personal contact details, whether intentionally or inadvertently, including sharing of location
- Breaching Data Protection and GDPR
- Breaching app or platform terms and conditions or legislation
- Risk of accounts accessed or 'hacked' by unauthorised people
- Isolation during COVID-19 has seen an increased risk of fraudulent activity, with offers of assistance such as online shopping, or the creation of fake platforms under the guise of existing platform names
- Facilitation of abusive or unkind behaviour and/or cyber-bullying between individuals
- Some people feel safe behind a screen and therefore may be more inclined to say inappropriate things, known as 'trolling'
- The disinhibition effect means participants may open up or make disclosures more rapidly, readily divulging personal content of a serious nature, this can have an impact on workers at the receiving end
- Unknown people joining conversations, friend requests from people unknown, 'Zoom bombing'
- Heightened risk to those suffering abuse should a harmer overhear pastoral conversations held with the victim

Section 4

4.0 Good Practice Guidelines

As with working face to face, there are ways to create and enable safer spaces online. You should maintain consistency between policies and approaches in the physical world and the online environment.

4.0.1 Code of Conduct

Where you have a Code of Conduct for your group, translate this into what they would look like when participating in online groups or interactions, this can be developed into an 'acceptable use' or guidance for online etiquette, for example:

- Ensure there is a nominated person with responsibility for online working and online safety
- Be mindful of the right to privacy

- Respectful modes of behaviour and language
- Appropriate physical presentation such as clothing
- Venue/environment – consider where participants are located; avoid using bedrooms or bathrooms. Consider if participants are in a private or shared environment
- Timing – consider when conversations are taking place, ensure they are at a suitable time for the people you are connecting with
- It is good practice to reiterate acceptable use and etiquette at start of group activities and to start the session by explaining the purpose of the call, video meeting or activity
- Consider if you can or should mix different age groups online
- Develop healthy boundaries – technology can lead us to feel we are accessible 24/7, whilst this may be necessary in limited cases, it may not be sustainable, having a clear outline of suitable contact times or activity plans can help us to maintain professional boundaries and keeps us mentally healthy too
- As in normal circumstances, contact with children, young people or vulnerable adults should take place with safely recruited, appropriately checked DBS workers (For a public church page, it is not considered to be used wholly or mainly by children and therefore you do not need the enhanced DBS with barring. You do, however, still need a DBS check).

4.0.2 Acceptable Use / Online Safety Agreement

Setting up an online safety agreement or acceptable use agreement can help ensure everyone remains safe and prevents issues arising whilst navigating the online world. An agreement should include positive statements and commitments about how you (the church) and those you are engaging with, can help to keep each other safe online.

It is a good idea to get those you are engaging with to help draw up the terms for an agreement.

To help you write an agreement, you should consider:

- Who to speak with when concerns arise
- What happens if someone does not follow the agreement
- How long the agreement is in place for

An example of an online safety agreement can be found at Childnet International by clicking **HERE** or from the NSPCC by clicking **HERE.**

4.0.3 Online Safety Policy

Although this document provides guidance on communicating and working with people safely online, it is not a policy. An online safety policy is recommended and should include:

- Roles and responsibilities, a named online safety lead, named safeguarding officers
- Training expectations and commitments
- Expected ways of communicating with people online, such as WhatsApp, Microsoft Teams, Zoom, Facebook
- Which online platforms have been agreed for use
- Consent and permissions (what level is needed for what and by whom)
- Codes of conduct and acceptable use
- Response to concerns, incidents of misuse and sanctions
- Guidance on risk assessing proposed online activities

An example of an online safety policy can be found at thirtyone:eight, by clicking **HERE**.

4.0.4 Profiles and Personal Accounts

Do not use your personal accounts, including email addresses or phone lines, use organisational profiles and devices wherever possible.

Many workers may assume their personal use of social media is personal. However, it is essential to recognise we are all role models, both on and offline. It is also important to be aware that once content is posted online it can no longer be considered private, as anyone who can see it, can copy and share without your knowledge or consent.

It can be a good idea to search for your name using public search engines such as Google or Bing to help identify any publicly available content such as social media posts, websites or images. If you see anything which is concerning, you should review your social media privacy settings, delete any inappropriate content, deactivate any old accounts or contact the relevant person or websites involved and request assistance in removing content.

Workers should also be mindful of commenting on friend's 'walls' or on any public news stories as this may be visible by others. It is recommended all content shared online is limited to 'friends' only, however professionals must be aware it is best to treat all information posted online as being potentially permanent and public.

It is recommended workers do not list their place of work on their social networking profile as this increases the risk of being identified.

Workers should not add or accept requests to virtually connect or 'friend' with children, young people, parents or carers or other persons where your relationship is of a professional capacity on any personal digital services. It is fine to be friends with your own children or Godchildren, for example. Accepting them on your personal social sites, could mean you are vulnerable as you will be sharing personal information or having access to personal information about those you are supporting. You may be leaving yourself open to allegations of inappropriate contact or conduct or find yourself exposed to unwanted contact.

Any pre-existing relationships or exceptions between children or parents, which may compromise this (for example if you are friends with a pre-school parent), should be discussed with your supervisor. This will ensure the relationship is formally acknowledged and enables transparent working.

If a young person turns 18 and becomes a leader, they should unfriend any young people under 18 that are involved in their youth group and follow the guidance for group leaders. This is part of forming new boundaries as a leader.

Consideration should always be given as to how this type of communication might appear to a third party. Compared with face-to-face working, the use of technology inevitably increases the potential for messages to be seen out of context or misinterpreted.

4.0.5 Devices and Passwords

Suitably protect devices e.g. by setting a PIN, password or passcode to prevent accidental or deliberate misuse. These should be strong, secure and use a mixture of lower and upper case letters, symbols and numbers. These codes should not be shared with others or written down and should be changed regularly. You should avoid word or number sequences e.g. password, 1234 etc. as they are easy to guess. It is recommended different passwords be used on different systems so if one account is compromised, others will remain secure. Using strong PINs, passwords and codes will help prevent other people from accessing your accounts and can help to prevent identity theft.

Workers should also be aware, for some devices, information and apps may still be accessed, even if a phone is locked. Ensure appropriate settings are applied to devices to restrict this. For example, iPhones can allow users to take photos on the device even when the screen is locked.

Ideally, avoid the use of personal equipment/devices and use ones provided by your church, circuit or district. One potential danger is allegations of an adult taking inappropriate photographs. A personal camera is more difficult to prove this was not the case. With organisation, equipment there is at least a demonstration the photography was consistent with policy.

4.0.6 Call Set-Up & Admin

Plan activities, meetings and calls, ensure the organiser has the ability and knowledge of how to mute/block/remove participants in the event they are displaying or sharing anything unsuitable or illegal, spend time getting to know the platform and its privacy settings.

Always use a secure, encrypted connection and password protect meetings and online activities to prevent unwarranted access. Zoom for example has the option to require a password to enter the meeting.

Think about the background of your video calls, is there anything that would give away personal details.

Consider sanctions for those breaching online etiquette or acceptable use guidelines.

Consider whether participants can control their environment i.e. switch off cameras and microphones.

If using online video clips, workers must ensure the video is clear of any unsuitable content (including links and adverts). Check you have the required consent and copyright permissions before publishing work publically.

Ensure participants know what to do, what is expected of them and who to speak to in the event of inappropriate contact or have concerns over content, if applicable; ensure parents have this information too.

4.0.7 Children & Parental Consent

Be aware of children in care or those known to children's services; ensure their locations cannot be determined.

Respect the minimum age requirements for social media and video chat enabled platforms. Do not invite young people to register for apps, software or platforms, which are not age-appropriate for them. For example, you have to be 13 years of age to have a Facebook account.

Contact parents/carers of those under 16 years; inform them of your intention to create a virtual meeting group. Seek their support and permission to do this. Explain how, when and where the meeting will be happening so everyone is clear about how it will take place. Encourage parents/carers to talk with their children about these arrangements. It is essential they are on board and willing to be a supervisory presence during group meeting times. Let everyone know you will remain in touch with parents and carers between meetings so they are fully informed of what will be happening. Underline that, you will have no direct contact with children or young people outside of the virtual group meeting or activity.

You will need parental consent to include their child in any virtual meeting space – the processes outlined **HERE**, if correctly followed, will include this.

Create a simple form within the text of your email for parents/carers to complete and return via reply. The form should include the following wording:

> *"I give consent for my child/children [insert name(s)] to participate in [insert platform, i.e. Zoom] meetings with their [i.e. youth group and youth leaders etc.]. I understand [the youth leaders] will follow Methodist Church safeguarding protocols at all times. I understand that I need to discuss with my child their participation in the [insert platform i.e. Zoom] meeting and agree any boundaries to their participation that I feel are appropriate."*

You may want to include some time when parents and carers are present (especially when meeting with under 11 year olds) so they are actively involved for part of the time and observers during the rest if they wish. As time goes on you may wish to consider asking your young people to take a lead and inviting them to create a space for meeting that is more peer led.

It is good practice to ask children and young people, who have the capacity, to make their own decisions whether they want to be involved in an activity. Most young people over 12 are likely to come into this category, although an assessment must be made, based on their individual needs. Consent from young people is not a replacement for parental consent. It is a way for the child or young person to be involved in the decision making process.

If the young person is 16 or above and living independently/is estranged from their parents then the form must be signed by the young person and a social worker/youth work/appropriate adult.

Consent forms will need to be filled out annually.

4.0.8 When a parent or carer is not willing to give consent for an activity

If a child or young person is keen to take part in an activity but their parent/carer is not willing to give consent, talk to the parent or carer so you can understand the reason for their objection. Discuss whether there is anything you can do to make the activity more suitable for the child (for example providing extra supervision/support). Suggest other activities the child could participate in, which parents/carers may be more comfortable with. Support parents in explaining to the child why they are not comfortable with their child taking part in the activity.

4.0.9 Group Calls / Video Meetings / Online Activities / Messaging

In order to minimise risk, always consider whether using group communication can achieve the same outcome rather than one to one.

You should not have one to one calls with a child or young person or vulnerable adult, if this is necessary, ensure you have two safely recruited workers to monitor the interaction and log the details of the contact.

Ensure you 'arrive' to the session or meeting before participants do, use 'waiting rooms' where available. 'Lock' the rooms if you can to prevent unwanted guests joining.

When messaging people using an online platform, ensure there are two, DBS checked admins set up on the feed. Facebook messenger, Instagram and WhatsApp all have the facility to have two admins.

It is recommended that you do not record the meeting. Most video conferencing software allows session hosts to record the goings on, but this would require separate permission for data capture and there are additional issues around storage, GDPR etc. Advise participants to not take photos or screenshots, or record (including with a secondary device). Turn off the ability to record if the platform you are using enables this.

Never reveal the full identity of individual participants and be sensitive to the needs of those who may have child protection or adult safeguarding concerns. Remind participants not to share personal information and not to respond to contact requests from people they do not know. Avoid using full names or 'tagging' people. Even with tagging turned off, others can still tag in the comments sections; if this happens, remove the tag to avoid anyone viewing to then have direct access to the person's profile.

When working face to face, friendly verbal banter between workers and participants may not be inappropriate, but it might look very different if carried out virtually and might lead to difficulties if misinterpreted, forwarded or used out of context.

4.0.10 Livestreaming

There are additional factors to consider when livestreaming:

- Ensure those involved are aware that live streaming is actually live. Any comments made will be seen by others and you will not be able to delete or edit them.
- Ideally, you should restrict the audience, for example by asking them to create a login and password.
- Consider whether other people will be able to reproduce and distribute your stream.
- If you are taking part in someone else's livestream make sure you know what content will be used in the stream and check it will be appropriate for the people watching it.

- Find out how the stream will be used in the future, for example if it will be archived or broadcast again.
- Some live streams request donations from the audience. Explain to participants that they do not have to contribute.

4.0.11 Record Keeping / Monitoring

Ensure a written record is kept of all one to one video calls, virtual meetings and online activities held and the content covered in each one; include list of attendees, length of call or activity.

Please be aware of 'live' feeds/chats such as those on Instagram and Snapchat that are automatically deleted after a period and avoid using these.

The General Data Protection Regulation (GDPR) and Data Protection Act (2018) outline the rights of individuals regarding information held and used by organisations. Many of the provisions, which were previously within the Data Protection Act 1998, are also present within GDPR and new Data Protection Act but the requirements for transparency have increased, along with the sanctions for failing to comply. Everyone within the church should understand their responsibilities under GDPR and comply with its requirements. Data must be processed:

- Fairly
- Transparently
- For a specified, explicit and legitimate purpose
- Adequate and limited to what is necessary
- Accurately and kept up to date
- For no longer than necessary for the specific purpose
- Securely

All workers are strongly advised to ensure they understand the Methodist policy regarding data protection and GDPR compliance, ***which can be found HERE and retention schedules can be found HERE.***

Also signpost participants to the platform's own privacy notices. Apps and other platforms typically have their own privacy notices, this means another company or organisation is likely to hold participant's personal information and have their own reasons for processing separate to the Methodist Church.

All personal information, including images, must be kept secure at all times. The storage of data on a hard disk or memory stick and transfer by email or other means is insecure. Making such storage secure may include password protection,

encryption of data and locking the computer when not in use. Risks including mislaying a memory stick, mistyping an email address, saving confidential files on a shared computer and laptop theft from a vehicle are all too common. Workers should consider approaches such as not storing information unless necessary and always deleting files (not just placing them in the recycle bin) after use.

Professionals should be aware that 'cloud' computing may not be appropriate for all uses, especially where security of confidential data and personal data is involved and should not be used unless it fully meets Data Protection Act and GDPR requirements and is suitably encrypted. Some services e.g. Google Drive, Dropbox, iCloud etc. do not always store data within the EU (they may have signed up to 'safe harbour' agreements but this may not always be sufficient) so it would not be advisable to use cloud storage hosted outside of the EU to store any content or files, which would be considered confidential or, which may be subject to the Data Protection Act i.e. contains personal information.

4.0.12 Domestic Abuse

For some, home is not a safe space. It is important to recognise factors such as the Coronavirus, unemployment, alcohol, drugs do not **cause** abuse to occur, however heightened anxiety and stress is likely to increase abuse in families where it is already being perpetrated. It should be noted that perpetrators might use factors such as the Coronavirus, to increase control over their partners or families.

If you are concerned about, or have already been supporting someone, you may wish to check in with him or her. If making contact by phone you should **always assume the harmer is listening in**. The same applies for instant messaging services, emails and any other platform used for communications.

It is advisable to have a readily thought out phrase to allow the victim or survivor to safely terminate a call, for example "if it is not safe to speak right now, then repeat after me "I'm sorry there's no one called Tina here, you must have the wrong number"".

Similarly, a coded word or phrase can be used in case of interruption, for example "no, sorry I'm not interested in taking part in the survey". The same can be applied should they wish you to contact emergency services.

Always be guided by the person you are supporting.

4.0.13 Prevent

The Prevent strategy, published by the Government in 2011, is part of our overall counter-terrorism strategy, CONTEST. The aim of the Prevent strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism. In the Act, this has simply been expressed as the need to "prevent people from being drawn into terrorism".

The 2011 Prevent strategy has three specific strategic objectives:

- Respond to the ideological challenge of terrorism and the threat we face from those who promote it
- Prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support
- Work with sectors and institutions where there are risks of radicalisation that we need to address.

The threats we are seeing take many forms, not only the high profile incidents of those travelling to countries such as Syria and Iraq to fight, but on a much broader perspective also. The internet, in particular social media, is being used as a channel, to not only promote and engage, but also, as a command structure.

Often this promotion glorifies violence, attracting and influencing many people including children and in the extreme cases, radicalising them. Research concludes that children can be trusting and not necessarily appreciate bias that can lead to them being drawn into these groups and adopt these extremist views, and in viewing this shocking and extreme content may become normalised to it

This threat is not just from groups, such as Islamic State, but from 'far right' groups also.

We are perhaps more familiar with this 'grooming' process and the risks posed to children by older young people and adults who form relationships with children to ultimately abuse them – the process is similar and exploits the same vulnerabilities.

It is for this reason that we recommend churches and circuits:

- Consider and discuss the threats from radicalisation and extremism for their children
- Ensure that addressing Radicalisation is effectively embedded in safeguarding practice and that PREVENT coordinators are engaged and signposted
- Consider how the threat of Radicalisation through the Internet and Social Media is being addressed
- Review how the above points are being addressed
- Review e-safety education in the light of these widening and extreme risks

Section 5

5.0 Reporting Concerns

You should ensure everyone is aware of who the Local Safeguarding Officers are and how to contact them in order to discuss concerns. If you are unable to contact your **District Safeguarding Officer**, get in touch with the Safeguarding Casework Supervisor who covers your District, these details can be obtained by contacting the District Office.

Having a link to the Child Exploitation & Online Protection Centre (**CEOP**) or agencies such as **Childline**, **NSPCC**, **ageUK** etc. ensures children, young people and vulnerable adults can report anything they are concerned about or seek advice in regards to the behaviour of a worker toward them.

If a person discloses online (or cyber) bullying to you, support and reassure them they have done the right thing by reporting the bullying. You should advise them how to deal with bullying appropriately, for example how to block bullies or report the users to the website. They should be instructed to keep evidence by taking screenshots or keeping messages (including times, dates, names and locations if possible) and to not retaliate. If it is a child, they may need support in telling their parent/carer. Incidents should be reported via the relevant online platform being used. If the bullying amounts to a crime, the option of reporting the incident to the police should be explored with the person on the receiving end, if they wish to pursue this course of action they should be supported in doing so.

Dealing with disclosures about online abuse should be responded to in much the same way as offline disclosures, although in some cases, additional queries about sites and services involved or collection of evidence will be required or recommended. Do not attempt to handle online abuse situations alone. You should write down the disclosure as soon as possible and using the person's own words.

Follow the Methodist Church policies and procedures if a person makes a disclosure. You should ensure you do not promise confidentiality and must explain what you are going to do with the information they have shared with you and why. Workers are often cautious of asking questions; however, in some cases it may be appropriate, for example if you need to clarify information i.e. 'Tell me…, Explain what…, Describe how…'.

Do not ask questions to gather opinions (i.e. why did you do that?) as that can people feel they are to blame. Workers must never request that a person prints, saves or forwards any images or content, which is thought to be an indecent image of a child.

The person should be reassured and supported at all stages and involved as far as is possible (according to their age and ability), for example speaking to

safeguarding officers, reporting concerns or speaking to parents/carers where appropriate.

If you believe there is evidence of safeguarding misconduct by worker, paid or otherwise, this must be reported to the **District Safeguarding Officer**.

You may wish to consult your local authority; LADO, Children's Services, Adult Social Care or the Police, if appropriate.

If inappropriate material is discovered reassure the participant, log and report the URL to a safeguarding officer or via online reporting tools. Workers should avoid printing or capturing any inappropriate material and must not print, forward or save illegal content.

Any inappropriate posts by children or young people or leaders to a group should be removed by the admin/s of the site. The reasons must then be explained to the person who posted the content. Examples of inappropriate post content could be:

- Racism
- LGBT+-phobia
- PREVENT issues
- Mental health worries
- Explicit personal images

If someone says something that concerns you and they are part of an online group, encourage them to stay online after the meeting or arrange to speak with them away from the wider group, so you can obtain further information and decide if any further action needs to be taken. Again, you need to make sure there are two safely recruited adults present for the conversation – perhaps one asking question and the other taking comprehensive notes. Follow safeguarding procedures as you would at any other time and consult your safeguarding officer and if appropriate, safe and applicable, the parents or carers as soon as practicable.

Section 6

6.0 Definitions

6.0.1 Online Safety

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

6.0.2 What is classed as 'inappropriate'?

Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate and illegal' and 'inappropriate but legal'. All staff should be aware that in the former case accessing illegal content investigation might lead to criminal investigation, prosecution, dismissal and barring. In the latter, it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

6.0.3 Inappropriate

Think about inappropriate in respect of your professionalism and being a role model. The scope for inappropriate content and behaviour is enormous, but bear in mind those actions outside of the workplace could breach the trust and confidence placed in the worker and may constitute misconduct.

6.0.4 Illegal

- Accessing (viewing), making, storing (possessing) or disseminating indecent images of children on or off the internet, whether on or off work premises is illegal. If proven, this will lead to criminal proceedings and the individual being barred from working with children and young people.

- Possessing or distributing indecent images of a person under 18 can include viewing such images online; this may also constitute possession even if they are not saved. What is regarded as indecent would ultimately be down to a jury to decide. The police have a grading system for different types of indecent image. Remember that children and young people may be harmed or coerced into posing for such images and are therefore victims of child sexual abuse and exploitation.

- This also applies to indecent images created by children and young people (those aged under 18) themselves and is often referred to as "sexting".

- Staff must **NEVER** print, save, forward etc. anything they suspect to be an indecent image of a child. Devices and systems thought to contain indecent images should be immediately secured or contained and police advice should be sought.

- Sharing adult pornography with children (under 18) is also illegal.

- The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets them or travels to meet with them anywhere in the world with the intention of committing a sexual offence.

- Illegal Hate / Harm / Harassment:
    - General: There is a range of offences to do with inciting hatred based on race, religion, sexual orientation etc.
    - Individual: There are particular offences to do with harassing or threatening individuals – this includes cyber bullying by mobile phone, social networking sites etc. It is an offence to make credible threats or send offensive messages with the purpose of causing the recipient distress or anxiety.

Please be aware that this list is not exhaustive and advice should always be sought if workers suspect a criminal offence has taken place

6.0.5 Prevent

The Prevent strategy, published by the Government in 2011, is part of our overall counter-terrorism strategy, CONTEST. The aim of the Prevent strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism. In the Act, this has simply been expressed as the need to "prevent people from being drawn into terrorism".

Section 7

7.0 Additional Sources of Support:

- **Kidscape** – National charity providing range of resources for those working with young people.
- **YoungMinds** – National charity supporting the mental health of young people.
- **ChildNet International** – Non-profit organisation working to help make the internet a safe place for children.
- **CEOP** – Multi-agency service dedicated to tackling the abuse and exploitation of children in the real and "e" world.
- **Thinkuknow** – A key focus of CEOP strategy to teach young people, professionals and parents/carers about e-Safety and has a "Click CEOP" report abuse button to report online abuse or suspicious behaviour.
- **IWF** – UK hotline for reporting illegal online content – this may be child abuse images, or material considered to be criminally obscene or inciting hatred.

- **ChildLine** – Children and young people can ring ChildLine on 0800 1111 to speak to someone in private. The ChildLine website offers excellent help and advice on a whole range of issues, for example online safety, sexting, grooming and bullying.
- **NSPCC** – Work to protect children and prevent abuse so we can make child abuse a thing of the past. Call the helpline on 0808 800 5000 to speak to someone ***[…]***
- **SWGfL** – Charity ensuring children benefit from technology, free from harm.
- **Digital Candle** – Charity Advice.
- **Catalyst** – Online beginner guides for using digital software.
- **Kelsi** – Online resource for education professionals in Kent.
- **UK Safer Internet Centre** – Promotes the safe and responsible use of technology for young people.
- **ParentPort** – Run by the UK's media regulators who set and enforce standards across the media to protect children from inappropriate material.
- **Stop it Now!** – A child sexual abuse prevention campaign run by the Lucy Faithfull Foundation.
- **Marie Collins Foundation** – A UK charity that aims to enable children who suffer sexual abuse and exploitation via internet and mobile technologies to recover and live safe, fulfilling lives.
- **Action Fraud** – A central point of contact for information about fraud and financially motivated internet crime.
- Find your local authority by **here.**
- ***[…]***
- View Government guidance on PREVENT **here.**
- Report terrorism **here.**
- For more information about the Home Office's radicalisation awareness training product Workshop to Raise Awareness of Prevent (WRAP) email **WRAP@homeoffice.x.gsi.gov.uk**