****

**E-SAFETY – SOCIAL MEDIA GUIDANCE**

**for people who work with Children and Young People**

## Contents

What do we mean by Social Media 3

Introduction 3

Background 3

Legal Consequences 4

Recent Case Law 5

General Guidelines 6

Social Networking (e.g. Facebook / Twitter) 7

Email 8

Images 9

Mobile Phones 10

Live Streaming Media (e.g. Web-cams, Skype etc.) 11

Using the Internet 12

Summary of Good Practice Guidelines 13

Template for Development of Organisational Media Policy 15

Reporting concerns about possible online abuse 15

Sources of Information 16

***What do we mean by Social Media?***

The term Social Media is used in a number of ways, but for the purposes of this guidance, is defined as any electronic communication that enables people to stay in touch online. Social Media includes web and mobile based technology which are used to turn communication into interactive dialogue between organisations, communities and individuals. Social media provides support for sharing information, images and making contact with people who may share a common interest.

***Introduction***

The purpose of this guidance is to clarify the professional responsibilities of staff working across services in children’s safeguarding and care delivery service for GCC and GCC’s responsibilities to its staff in relation to the increasing use of social media. This should be read in conjunction with the GCC Social Media Policy. This document is guidance only, it is not intended to interfere in an employee’s private life, but to help avoid work and private lives clashing in inappropriate ways because of social networking activities. It should be read in conjunction with the relevant policy within your own employing organisation.

***Background***

Digital technology has become an important part of everyday life and offers exciting opportunities. However there have been a number of incidents where staff safety could have been compromised because of service users gaining access to their private social media accounts. This has led to a need for clear practice guidance for workers and organisations around safer working practice in this area.

As someone who works with children and young people, or adults who are their parents and carers, whenever you are operating in the digital world you must always have your professional role in mind and always consider how your behaviour could affect your professional reputation and employment as well as the safety of yourself and your family. **All digital records should be considered to be permanent.**

**Please use the following pages as guidelines. They have been developed to help you to use social media safely.**

***Legal Consequences***

There can be legal consequences attached to the inappropriate use of those services.

**Offences Committed on Social Networking Sites,**

**Email, Mobile Technology & the Internet**

**Threats to kill**

Conviction of a Summary Offence: A fine and/or a maximum of 6 months imprisonment

Conviction of an Indictable Offence: 10 years in prison

**Intended harassment of another person**

Conviction of a Summary Offence: A fine and/or a maximum 6 months in prison

**Putting a person in fear of violence**

Conviction of a Summary Offence: A fine and/or maximum of 6 months in prison

Conviction of an Indictable Offence: A fine and/or a maximum of 5 years imprisonment

**Intending to cause distress or anxiety by sending indecent, offensive or threatening letters, electronic communication or other articles to another person**

Conviction of a Summary Offence: A fine and/or maximum of 6 months in prison

**Threats to destroy or damage property**

Conviction of a Summary Offence: A fine and/or a maximum of 6 months imprisonment

Conviction of an Indictable Offence: 10 years in prison

**Causing intentional harassment, alarm or distress**

Conviction of a Summary Offence: A fine and/or maximum of 6 months in prison

*Summary offences include less serious offences. (Magistrates' Court).*

*Indictable offences are more serious. (higher court by a judge and jury).*

## General guidelines –

* Remember you are responsible for the data on your electronic communication device
* DO NOT behave in a way that could suggest that you are trying to develop a personal relationship with a child or vulnerable adult
* DO NOT post any content that could be deemed defamatory, obscene or libellous
* DO NOT post comments that exhibit or appear to endorse grossly irresponsible behaviour or law breaking of any kind

**🗷 Inappropriate**

1. Give your personal information to service users -children/ young people, their parents/ carers. This includes mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords etc.
2. Use your personal mobile phone to communicate with service users. This includes phone calls, texts, emails, social networking sites, etc.
3. Use the internet or web-based communication to send personal messages to children/young people
4. Share your personal details with service users on a social network site
5. Add/allow a service user to join your contacts/friends list on personal social networking profiles.
6. Use your own digital camera/ video for work. This includes integral cameras on mobile phones.
7. Play online games with service users.

**🗹 Appropriate**

1. Set your privacy settings for any social networking site.
2. Ensure any technological equipment, (including your mobile phone) is password/ PIN protected.
3. Consider having professional online accounts/ identities if you wish to have online contact with service users, their families and other professionals.
4. Make sure that all publicly available information about you is accurate and appropriate
5. Remember online conversations may be referred to as ‘chat’ but they are written documents and should always be treated as such.
6. Make sure that you know the consequences of misuse of digital equipment.
7. If you are unsure who can view online material, assume it is public. Remember - once information is online you have relinquished control.
8. Switch off Bluetooth
9. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.

 We recommend the above as good

practice, these will be subject to management approval and local organsiational policies.

For fuller statements go to P13 & 14

***Social Networking***

Facebook and Twitter are the most well known packages but other packages include BEBO (Blog Early, Blog Often), MySpace, Yahoo, LinkedIn and MSN. These are not exhaustive. Remember: **Host privacy settings often change – keep track of yours**.

Make sure your security settings are not open access - set to family and friends only

Don’t accept people you don’t know as friends – they could be service users. Go for quality not quantity.

Be aware that belonging to a ‘group’ can be a ‘back door’ into your profile.

Ask your family and friends to protect your professional status and not post tagged images of you on their open access profiles

Set your privacy settings so that you have to pre-approve any tagged photos.

Don’t use your personal social network profile to communicate with or share images or take images of children/ young people and their parents/ carers

*Either using your personal or organisational equipment*

Don’t accept children and young people/ parents and carers as friends on your personal page.

Safe practice

You have an open access profile that includes inappropriate personal information and images e.g. holiday snaps, hen nights

You accept service users as friends on your personal profile once work is completed. Other service users may gain access to your profile.

You collect ‘friends’ including people you don’t know in real life.

You use your personal profile to communicate with service users without your manager’s knowledge or permission.

Poor practice

## Email

Don’t use your personal email account to communicate with children/ young people, their parents/ carers and adults who may be at risk or put you at risk

*Either via mobile phones or web based software*

Use your GCC email for all of your professional communications.

Best practice

Check your organisation policy regarding use of your work account for personal use e.g. shopping.

This is in the GCC social media policy on staff net

Poor practice blurs the professional boundaries and can make workers vulnerable to bullying/ harassment/ allegations. It may result in capability/ disciplinary proceedings

Safe practice

You use your personal email account to communicate with service users and their families without manager’s knowledge or permission.

You retain emails for your personal use.

Poor practice

## Images (still and moving)

Your organisation should provide equipment for you.

Know who/ where to get equipment from.

Don’t use your own equipment to take images of children/ young people

*This includes built in equipment on personal mobile phones, standalone cameras/ video recorders.*

Best practice

Senior managers agree you can use your own equipment.

You make arrangements for pictures to be downloaded to organisation network immediately after the event.

Safe practice

May result in capability/ disciplinary proceedings

You download images from organisation equipment to your own equipment.

You use your own equipment without manager’s knowledge or permission.

You retain images for your personal use and don’t delete them from your equipment.

Poor practice

## Mobile Phones

Don’t use your personal mobile phone to communicate with children/ young people, their parents/ carers and adults who may be at risk.

*This includes phone calls, text messages, email or web-based communications e.g. Twitter*

You should use your work mobile, or have access to a work mobile.

Make sure you know about inbuilt software/ facilities and switch off if appropriate

Best practice

Service users having your personal details may make you vulnerable to harassment or bullying

You use your own equipment without manager’s knowledge or permission.

You retain service user contact details for your personal use.

Poor practice

 Workers may be vulnerable to allegations as well as capability/ disciplinary process

## Live Streaming Media

For example Web cams or video conferencing. Facetime and Skype are the most well known packages but there are many more packages in development, Therefore these are not exhaustive.

Don’t use your personal web-cam to communicate with children/ young people, their parents/ carers or to make a record of activity without permission

Make sure you know about inbuilt software/ facilities and switch off.

Best practice

Workers may be vulnerable to allegations as well as capability/ disciplinary process

You use your own equipment without manager’s knowledge or permission.

You retain service user information/ activity for your personal use.

Poor practice

## Using the Internet

Appropriate software to ensure safe and secure access to the web is installed

Understand how to search safely online and how to report inappropriate content either via your organisation’s ICT section or via the CEOP report button

Be aware of the organisation policy for the use of the internet on your work computer.

Security software may mean that some sites are blocked or restricted access.

Best practice

Be aware that the organisation’s monitoring software will log your activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Safe practice

Accessing or downloading inappropriate or illegal material may result in criminal proceedings.

Poor practice

## Summary of Good Practice Guidelines

* **APPROPRIATE**
1. Set your privacy settings for any social networking site to ensure only the people you want have sight/ access to the contents. Keep these updated. The default settings for most social networking sites are set to open access where anyone can see everything.
2. Ensure your mobile phone (any technological equipment) is password/ PIN protected. This will ensure that other people can’t use your equipment and get you into trouble.
3. Make sure that all information about you that is publicly available is accurate and appropriate – think particularly about whether photographs/ stories that you may have posted in your personal life are appropriate for a person with a professional life and a reputation to lose. If you don’t want it to be public, don’t put it online.
4. Remember that online conversations may be referred to as ‘chat’ but they are written documents and should always be treated as such. Be mindful about how you present yourself when you are publishing information about yourself or having ‘conversations’ on-line.
5. Make sure that you are aware of the GCC social media policy regarding the use of both organisational and personal digital equipment and the consequences of misuse. Breach of the policy can result in capability/ disciplinary actions by your employer, professional body and criminal proceedings by the police.
6. Err on the side of caution. If you are unsure who can view online material, assume that it is publicly available. Remember - once information is online you have relinquished control of it. Other people may choose to copy it, to edit it, to pass it on and to save it.
7. Switch off any Bluetooth capability any device may have installed as standard. Bluetooth allows another person to have access to your equipment – they can then pretend to be you.
8. Always be aware that technology is constantly upgrading and improving. You may have access to websites via a work-provided smart phone that are blocked by your computer. Mobile phones come with locator software. Cameras can be a feature of games consoles. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.
* **INAPPROPRIATE**
1. Give your personal information to service users i.e. children/ young people, their parents/ carers. This includes personal mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords/ PIN numbers etc.
2. Use your personal mobile phone to communicate with service users i.e. children/young people or parents/carers either by phone call, text, email, social networking site.
3. Use the internet or web-based communication to send personal messages to service users i.e. children/young people, parents/ carers.
4. Share your personal details on a social network site with service users i.e. children/young people, their parents or carers. This includes accepting them as friends. Be aware that belonging to a ‘group’ may give ‘back door’ access to your page even though you have set your privacy settings to family and friends only.
5. Add/allow service users i.e. a child/young person, their parents/ carers to join your contacts/friends list on personal social networking profiles.
6. Use your own digital camera/ video for work. This includes integral cameras on mobile phones.
7. Play online games with service users i.e. children, young people, their parents or carers. This can be difficult when the culture is to play with ‘*randoms*’. Check out before you play online with someone you don’t know.

##

## What to do if you have concerns

As a user of social networking site, you may at some time have a concern about what you are seeing or being told about by another user. Concerns may range from negative or abusive comments and cyber bullying to suspected grooming for sexual abuse.

## Reporting concerns about possible online abuse

All staff should be familiar with your organisation’s reporting procedures which should include the reporting of potentially illegal/abusive content or activity, including child sexual abusive images and online grooming.

In addition to referring concerns to your organisation’s designated person, you should immediately report online concerns to the Child Exploitation and Online Protection Centre (CEOP) or the police, in line with internal procedures. Law enforcement agencies and the service provider may need to take urgent steps to locate the child and/or remove the content from the internet.

In the UK, you should report illegal sexual child abuse images to the Internet Watch Foundation at www.iwf.org.

Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre at www.ceop.uk.

***Where a child or young person may be in immediate danger, always dial 999 for police assistance.***

***Where to find further help***

There are several web sites which provide advice about how to manage your internet security, for example WikiHow

[www.safetynetkids.org.uk/personal-safety/staying-safe-online](http://www.safetynetkids.org.uk/personal-safety/staying-safe-online)

[www.kidsmart.org.uk](http://www.kidsmart.org.uk)