UK & INTERNATIONAL
HEALTH COACHING ASSOCIATION

Digital Security, Online Safety & Lone Working

Guidance for Health Coaches

UK & INTERNATIONAL
HEALTH COACHING ASSOCIATION

Digital Security, Online Safety & Lone Working

Guidance for Health Coaches

Contents

Part One: General Guidance on digital security & online safety

Please note that UKIHCA has collated this guide from a wide range of resources within the public domain and provides this information in good faith and as guidance only. **It is the responsibility of each individual to decide whether and how to use this information.**

To protect your identity online, you should follow these procedures:

Create a *Secure Digital Identity:* Health coaches should have a secure and verified digital identity that allows you to interact with clients without revealing personal information.

"Secure Digital Identity" refers to the process of establishing a unique representation of your identity on digital platforms. This is crucial and allows you to interact with clients in a secure and confidential manner.

Here's how verify your digital identity:

1. **Create a Digital Profile**: The first step is to create a digital profile on a secure platform such as isosconnect Booking app | Video consultation | isosconnect | United Kingdom. This could be a health coaching app or website. The profile should include professional details like qualifications, experience, and areas of expertise.
2. **Two-Factor Authentication (2FA)**: To enhance security, health coaches should enable two-factor authentication on their digital profiles. This means that in addition to entering a password, a second form of identification is required to access the account. This could be a code sent to a mobile device or an email.
3. **Privacy Settings**: Health coaches should ensure that their privacy settings are configured correctly to prevent the disclosure of personal information. They should only share information that is necessary for the coaching process.
4. **Secure Communication**: All communication with clients should be done through the secure platform. This ensures that personal information is not revealed and that conversations are confidential.
5. It's important to remember that **maintaining a secure digital identity is an ongoing process and requires regular updates and checks**.

Education and Awareness: Coaches should take steps to educate themselves about the risks and best practices for maintaining their online identity.

Use of Secure Platforms: Coaches should use secure platforms for delivering online coaching sessions. Ideally use a purpose-built platform that includes secure bookings, payments, email and video functions. If using separate specialist video platforms, they should have robust security

measures in place to protect the identities of both the coach and the coachee. Here are some available options-

- **Zoom**: Zoom is a popular video conferencing tool that offers end-to-end encryption for all meetings, role-based user security, password protection, waiting rooms, and place attendee on hold.
- **Microsoft Teams**: Microsoft Teams is a platform that combines workplace chat, video meetings, file storage, and application integration. It's part of the Office 365 suite and offers features like two-factor authentication and data encryption.
- **Google Meet**: Google Meet is a video-communication service developed by Google. It is one of the secure platforms for video conferencing as it encrypts all data and meetings.
- **Cisco Webex**: Cisco Webex is a company that provides on-demand collaboration, online meeting, web conferencing, and video conferencing applications. Its products include meeting and team collaboration software and accessories like headsets.
- **GoToMeeting**: GoToMeeting is a web-hosted service created and marketed by LogMeIn. It is an online meeting, desktop sharing, and video conferencing software that enables the user to meet with other computer users, customers, clients or colleagues via the Internet in real time.

WhatsApp or Face Time are commonly used, but because these systems are linked to your mobile number, it is recommended that you **do not use them unless you have a separate business pages version of the App or that you have a separate business phone number**, in which case, you should still follow these steps to ensure your security.

WhatsApp:

- **End-to-End Encryption**: WhatsApp uses end-to-end encryptions for all its messages, calls, photos, and videos. This means only you and the person you're communicating with can read what's sent, and nobody in between, not even WhatsApp
- **Two-Step Verification**: Enable two-step verification in your WhatsApp account settings for an added layer of security
- **Privacy Settings**: Make use of the privacy settings to control who can see your profile photo, status, and last seen status
- **Block Unwanted Contacts**: If you receive messages from unknown or unwanted contacts, make sure to block them
- **Secure Chats**: You can also secure your chats by setting a fingerprint lock.

FaceTime:

- **End-to-End Encryption**: Like WhatsApp, FaceTime calls are also end-to-end encrypted. This means they can only be accessed by the sender and receiver
- **Use Verified Contacts**: Only accept FaceTime calls from people you know and have added to your contact list
- **Private Apple ID**: Use an Apple ID for FaceTime that doesn't include personal information like your name or address

- **Strong Passwords**: Use a strong, unique password for your Apple ID to prevent unauthorized access

Remember, no matter what platform you use, it's important to stay vigilant and follow best practices for online security. This includes regularly updating your apps and operating system, being wary of unsolicited calls or messages, and not sharing sensitive information unless necessary.

Keep Your Personal Information Private:

- Be cautious about what you share online. Avoid posting sensitive details such as your home address, phone number, or other personal information on social media platforms
- Remove yourself from people search websites that might expose your data, for example:

Truthfinder: This is a people search engine that offers accurate information from a variety of sources. You can search for police records of an individual, check court records, photos from social media, contact information, and much more.

BeenVerified: BeenVerified is among the best sites to search for people you've lost contact with.

Intelius: Intelius is one of the most reputable people search websites - it's been around since 2003.

Instant Checkmate: This is another popular people search website.

USSearch: USSearch is a reliable platform for people search.

PeopleFinders: PeopleFinders is a good choice for searching for people.

Pipl: Pipl is another well-known people search website.

Limit Location Information:

- Refrain from posting real-time location updates. Broadcasting your whereabouts can make it easier for stalkers to track you
- Be cautious about sharing your location in posts or check-ins.

Be Selective with Friend Requests:

- Only accept friend requests from people you know and trust. Avoid adding strangers or suspicious accounts to your social media networks
- Remember that not everyone online has good intentions.

Use Strong Passwords:

- Create unique and robust passwords for your online accounts. A strong password includes a mix of uppercase and lowercase letters, numbers, and special characters
- Regularly update your passwords to enhance security.

Activate Two-Factor Authentication (2FA):

- Enable 2FA wherever possible. This adds an extra layer of security by requiring a second form of verification (such as a text message or authentication app) when logging in.

Tighten Social Privacy Settings:

- Only use the business pages offered by social media platforms for promoting your business. The most popular social media platforms offer this option: for example…

Facebook; How to create and set up a Facebook Page for your business | Meta for Business
YouTube; Create & Optimize Your Business Channel - YouTube Advertising - YouTube Advertising
Instagram; Getting started on Instagram for business | Instagram for Business
WhatsApp; Get started and download on the WhatsApp Business app | WhatsApp Business

Remember, each platform has its unique features and advantages, so it's important to choose the ones that align best with your business goals and target audience. Also, always ensure to follow each platform's guidelines when setting up and managing your business page.

Keep Your Devices Secure:

- Install and regularly update antivirus and anti-spyware software on your computer and mobile devices
- Cover your webcam when not in use to prevent unauthorized access

Software Updates:

- Keeping all software and applications up-to-date is crucial for security, install updates as they are notified by the provider.

Recognising 'red flags'

As a professional health coach, it's crucial to ensure the safety and integrity of interactions online. Here are some refined strategies to recognise and handle suspect contacts:

Technological Literacy: Learn how to manage privacy settings (see previous section) for each device and digital platform that you use.

Proactive Protection: Develop a proactive approach to guard against opportunistic unwanted behaviour that may be disguised as an initial contact. This includes implementing robust security

measures (see previous section) and utilising contact forms that require the submission of contact details, reason for contact and desired outcomes, all of which are barriers to unwanted contacts.

Awareness and Preparedness: Always be aware of the possibility of suspect contacts and be prepared and vigilant.

Standardised Contact Methods: Be wary of direct (and often persuasive) attempts to contact you outside your published preferences. Any deviation from this norm should be treated with caution.

Urgency: Be aware of new and unknown contacts that demand an urgent response. In general, an approach for health coaching support is *not* an urgent or immediate requirement. If using an online booking system, set a default for availability that is two days in the future. This will be a barrier and will discourage unwanted contacts.

Potential for Manipulation: Acknowledge the potential for manipulation. As coaches, the empathetic and non-judgmental approach can sometimes make you a target. Develop strategies to recognise and handle such situations. Decide what your Red Flags are and be prepared to close any contact when they occur.

Trust Your Instincts: Trust your gut instincts. If a contact or request seems unusual or makes you feel uncomfortable, you should say no or ignore it.

On-screen vigilance: Always insist on 'camera on' engagement. Remain aware of a client's verbal and on-verbal communication signals and any unusual requests. Do not hesitate to end the consultation immediately if you feel unsafe.

Support System: Contact Admin@ukihca.com to report suspect contacts and get the necessary help or guidance.

Protect yourself from cyberstalkers

Remember that cyberstalkers can be methodical and obsessive, so vigilance is crucial. If you suspect you're being stalked online, keep a detailed log of interactions and report them to the proper authorities

Dealing with an online stalker can be distressing, but there are steps you can take to protect yourself. Here's what you can do:

*Document **EVERYTHING**:*

- Keep a detailed record of all interactions with the stalker. Save screenshots, emails, messages, and any other evidence
- Note dates, times, and descriptions of incidents. This documentation will be crucial if you decide to involve law enforcement.

Block and Restrict:

- Block the stalker on all platforms where they're harassing you. This includes social media, email, and messaging apps
- Adjust your privacy settings to limit their access to your information.

Inform Trusted Friends and Family:

- Share your situation with close friends and family. They can provide emotional support and be aware of what's happening
- Avoid facing this alone; having a support system is essential.

Report to the Platform:

- Report the stalker's behaviour to the relevant platform (e.g., Facebook, Twitter, Instagram). Most platforms have mechanisms for reporting harassment
- Provide evidence and follow their guidelines for reporting.

Contact Law Enforcement:

- If the stalking escalates or becomes threatening, involve law enforcement
- File a police report and provide them with the evidence you've collected
- Obtain a restraining order if necessary
- Learn more about the police advice - Stalking and harassment | Police.uk (www.police.uk)

Secure Your Online Presence:

- Change passwords for all your accounts, especially if the stalker has gained access
- Enable two-factor authentication (2FA) for added security.

Be Cautious Offline:

- Be mindful of sharing personal information offline as well. Stalkers may try to gather details about your daily life
- Vary your routines and avoid predictable patterns.

Seek Professional Help:

- Consider talking to a counsellor or therapist. Dealing with a stalker can be emotionally draining, and professional support can be beneficial
- Reach out to organizations that specialize in stalking prevention and victim assistance.

Remember that your safety is the top priority. Trust your instincts—if something feels wrong, act. You don't have to tolerate harassment, and there are resources available to help you.

Harassment, abuse and intimidation

Although the terms Harassment, abuse and intimidation are often used interchangeably, they have specific social and legal meanings.

Referring to the Home Office and Department of Health guidance, The Local Government Association explains **abuse** as "a*s a single act or repeated physical, verbal or psychological acts that violate an individual's human and civil rights. Some cases of abuse constitute criminal offences. For example, physical, psychological or sexual assault, theft, fraud and gender and racial discrimination"*.

The Protection from Harassment Act 1997 indicates that someone's actions amount to harassment *"when they make the victim feel distressed, humiliated, threatened or fearful of further violence. The main goal of harassment is to persuade victims either not to do something that they are entitled or required to do or to do something that they are not obliged to do. Actions listed under the Protection from Harassment Act include but are not limited to: phone calls; letters; emails; visits; stalking; verbal abuse of any kind, including on social media; threats; damage to property; bodily harm. Such actions amount to harassment when they occur more than once.*

Public intimidation is defined as "words and/or behaviour intended or likely to block, influence or deter participation in public debate or causing alarm or distress which could lead to an individual wanting to withdraw from public life". This includes actions of abuse, harassment and intimidation such as: verbal abuse; physical attacks; being stalked followed or loitered around; threats of harm; distribution of misinformation; character assassination; inappropriate emails, letters, phone calls and communications on social media; sexual harassment or sexual assault; and other threatening behaviours, including malicious communications such as poison pen letters, indecent or grossly offensive emails or graphic pictures that aim to cause distress or anxiety.

Check what you can do about harassment HERE

Sexual Harassment

"*In England and Wales, the legal definition of sexual harassment is when someone carries out unwanted sexual behaviour towards another person that makes them feel upset, scared, offended or humiliated.*

It is also when someone carries out this behaviour with the intention of making someone else feel that way. This means that it can still be sexual harassment even if the other person didn't feel upset, scared, offended or humiliated"

Sexual harassment includes a very wide range of behaviours and some forms of sexual harassment are unlawful.

Everyone responds differently to sexual harassment (and other forms of sexual violence) – so whatever someone *feels* is a valid response.

You can get help and support after sexual harassment HERE

You can call report an incident to the POLICE by: dialing 999 (emergency); dialling 101 (non-emergency); reporting online; or by visiting your local police station.

Members who experience incidents of concern can alert UKIHCA HERE

General Guidance on digital security and safeguarding of Health Coach clients

In extreme cases, your clients' data could be at risk so have the following measures in place.

Confidentiality: Coaches should maintain strict confidentiality. Information acquired through coaching engagements should not be disclosed without the express or written permission of the coachee, unless required by law.

Data Protection: Coaches should adhere to the highest standards of data protection. Any data relevant to the coachee should be kept confidential unless required by law

Clear Contracts: At the start of a coaching engagement, a clear and easy-to-understand contract should be established. This contract should outline how coaching information will be used and should avoid promises of 'total' or 'absolute' confidentiality.

References

The information provided about digital safeguarding as a health coach aligns with general guidelines for digital safeguarding and the specific practices of health coaches.

Please note that while these sources provide general guidance, it's important for each health coach to tailor these guidelines to their specific circumstances and local regulations.

Always consult with a professional or legal advisor for personalised advice.

Stay safe!

Here are some sources that support this information:

Security; Expanding Secure Communication: Embracing the Challenge of Email Security for Health Coaches – CleanBox

Booking app | Video consultation | isosconnect | Psychologist | Counselling | United Kingdom

Two-factor Passwords - the easiest way to use passwords safely and securely (passwordcoach.com)

Advantages of Multi-Factor Authentication for Healthcare Organizations — HealthTech (healthtechmagazine.net)

Confidentiality; Confidentiality_in_Coaching.pdf (coachhub.com)

Cyberstalkers; 5 Effective Strategies to Protect Yourself from Cyberstalkers (digitalsecurityworld.com)

How to protect yourself against cyberstalking (bitdefender.com)

What is cyberstalking - Cyberstalker Protection (kaspersky.com)

Harassment; Stalking or Harassment | The Crown Prosecution Service (cps.gov.uk)

Part Two: Lone Working Guidelines for Health Coaches

Lone working is often an integral part of a health coach's role, especially when meeting clients in person. This guide aims to support health coaches to be prepared, safe, and confident when working alone.

Lone working refers to work activities conducted in isolation from other workers without close or direct supervision.

Please note that UKIHCA has collated this guide from a wide range of resources within the public domain and provides this information in good faith and as guidance only. **It is the responsibility of each individual to decide whether and how to use this information.**

Overview

Common Scenarios: Home visits, private coaching sessions, or community outreach programs.

Risk Assessment: Conduct a thorough risk assessment for each location where you meet clients. See below.

Check-In System: Establish a routine check-in system with a colleague or supervisor.

Emergency Contacts: Always have a list of emergency contacts readily available.

Pre-Meeting Checks: Confirm the meeting beforehand and ensure someone knows where you are.

Location Safety: Choose public or well-known locations for meetings when possible.

Client Screening: Have a client screening process in place to identify any potential risks.

Stay Connected: Keep a mobile phone with you for communication.

Distress Signals: Set up code words or distress signals with your team for emergencies.

Mental Health: Be aware of the mental toll lone working can take and have support systems in place.

Physical Health: Ensure you have access to first aid and know basic self-defense techniques.

Insurance: Ensure you have appropriate insurance coverage for lone working.

Professional Boundaries: Maintain professional boundaries and be aware of the legal implications of lone working.

Lone Worker Training: Participate in lone worker safety training programs.

First Aid Training: Regularly update your first aid training.

Lone working as a health coach requires careful planning and awareness. By following these guidelines, you can create a safer working environment for yourself and provide the best possible service to your clients.

Remember, the key to safe lone working is preparation and awareness. Stay safe and empowered in your role as a health coach!

Safety Apps

Utilise safety apps that can send alerts or track your location. Consider wearing a personal alarm or other safety devices. For health coaches or anyone needing to track location and send alerts, there are several apps that can provide these services with accuracy and reliability. Here are some available options:

- **Qustodio**: Offers **24/7 real-time location tracking**, geofencing, and a **Panic Button** feature for emergencies. It's highly rated for its accuracy and ease of use on both Android and iOS devices
- **Norton Family**: Known for its **super accurate and customizable location tracking** with set times for notifications, making it a good choice for professional use
- **Bark**: Provides **less invasive location-tracking features** which can help build trust with clients or family members while still ensuring safety
- **FollowMee GPS Tracker**: A robust app that enables real-time tracking of device locations and includes features like geofencing, location history, and alerts.

Please note UKIHCA takes no responsibility for the function of these Apps and provides this information in good faith as guidance only.

Risk Assessment for Lone Working Health Coaches

Lone working as a health coach involves unique risks. This assessment aims to identify potential hazards and implement preventive measures.

Hazard Identification

Consider the following hazards:

Physical Risks:

- **Assault or Violence:** Interacting with clients in unfamiliar environments may expose health coaches to physical harm
- **Accidents:** Trips, slips, or falls during home visits or outdoor sessions.

Health Risks:

- **Medical Emergencies:** Health coaches may encounter clients with sudden health issues
- **Infectious Diseases:** Exposure to contagious illnesses.

Environmental Risks:

- **Unsafe Locations:** Meeting clients in poorly lit or isolated areas
- **Extreme Weather:** Heat, cold, rain, or snow.

Psychosocial Risks:

- **Emotional Stress:** Dealing with clients' emotional issues
- **Isolation:** Loneliness and lack of support.

Risk Assessment Matrix

Assess the likelihood and severity of each hazard:

	Very Low Impact	Low Impact	Medium Impact	High Impact	Very High Impact
Very Low Likelihood	1	2	3	4	5
Low Likelihood	2	4	6	8	10
Medium Likelihood	3	6	9	12	15
High Likelihood	4	8	12	16	20
Very High Likelihood	5	10	15	20	25

In this matrix:

- The rows represent the likelihood of the risk occurring, from very low to very high
- The columns represent the potential impact of the risk, from very low to very high
- The numbers in the cells represent the risk score, which is a product of the likelihood and the impact. The higher the score, the higher the risk.

Use the matrix to assess the risk associated to all likely or possible scenarios.

High Risk: Assault, medical emergencies, extreme weather
Medium Risk: Accidents, infectious diseases, emotional stress
Low Risk: Unsafe locations, isolation

For any risks with a high likelihood and high impact, you need to prepare a plan or strategy and put measures in place that mitigate the risk to an acceptable level, or do not expose yourself to the risk at all.

Control Measures

Implement preventive measures:

Client Screening:
- Obtain relevant client information before meetings
- Assess potential risks (e.g., history of violence, mental health issues).

Communication:
- Maintain regular contact with a supervisor or colleague
- Use mobile phones or safety apps for real-time communication.

Emergency Procedures:
- Know emergency contact numbers
- Establish a protocol for medical emergencies.

Location Safety:
- Choose well-lit, public meeting places
- Avoid isolated areas.

Self-Defense Training:
- Learn effective self-defence techniques
- Carry personal alarms if necessary.

Health and Wellbeing:
- Prioritize mental health
- Stay physically fit
- Access first aid resources.

Review and Update

Regularly review and update this risk assessment:

- After incidents or near misses
- When working in new locations
- When regulations change.

References

The information provided about lone working as a health coach aligns with general guidelines for lone working and the specific practices of health coaches. Here are some sources that support this information:

1. **Lone Working:** The Health and Safety Executive (HSE) in the UK provides guidance on lone working, which includes conducting risk assessments, providing training, and maintaining regular communication
2. **UKIHCA Guidelines:** The UK & International Health Coaching Association (UKIHCA) sets the scope of practice for health coaches, which includes working with individuals in a client-centred process to facilitate and empower the client to develop and achieve
3. **Safety Apps**: Several safety apps are available that can help lone workers stay safe. These apps offer features like real-time location tracking, panic buttons for emergencies, and check-in systems
4. **Risk Assessment**: Conducting a risk assessment is a crucial part of ensuring the safety of lone workers. This involves identifying potential hazards, assessing the likelihood and severity of each hazard, and implementing preventive measures.

*Please note that while these sources provide general guidance, it's important for each health coach to tailor these guidelines to their specific circumstances and local regulations.

Always consult with a professional or legal advisor for personalised advice.

Stay safe!

Click the links to learn more:

hse.gov.uk
ukihca.com
safetyculture.com
aware360.com
safepointapp.com
healthassured.org
peninsulagrouplimited.com
suzylamplugh.org
staysafeapp.com