ICPHAA

Irish Counselling, Psychotherapy & Allied Healthcare Professionals Association

MEMBERS' PROFESSIONAL PRACTICE

Digital & Practice Environment Policy

The standards ICPHAA members follow when working online or by telephone, using technology and social media, and providing a safe, private physical space for clients.

REFERENCE	ICPHAA-POL-06	VERSION	1.0
EFFECTIVE	9 November 2026	NEXT REVIEW	9 November 2027
POLICY OWNER	ICPHAA Board of Directors		

MEMBERS' PROFESSIONAL PRACTICE · ICPHAA-POL-06

Digital & Practice Environment Policy

APPLIES TO	All ICPHAA members who see clients in person, online or by telephone, or who use digital technology or social media in their professional work.
VERSION	1.0 · effective 9 November 2026 · next review 9 November 2027
POLICY OWNER	ICPHAA Board of Directors
CONTACT	ICPHAA Registry · admin@icphaa.ie

AT A GLANCE

- Members assess each client's suitability for online or telephone work before it begins and agree an emergency plan.
- Only secure, encrypted platforms that comply with the GDPR and the Data Protection Acts 1988–2018 are used for client work.
- Basic cybersecurity is an ethical duty: strong passwords, multi-factor authentication, updated devices and encrypted storage.
- Members do not connect with current or former clients on personal social media.
- Physical practice rooms are private, safe and accessible, whether in shared premises or at home.

CONTENTS

1 Purpose 3
2 Scope 3
3 Suitability and consent for remote work 3
4 Platforms and data protection 4
5 Emergency and risk protocols 4
6 Cybersecurity, communications and digital records 5
7 Social media and online boundaries 5
8 The physical practice environment 6
9 Responsibilities and breaches 6
10 Monitoring and review 6

1. Purpose

Counselling and psychotherapy are now delivered in many ways: in person, by video, by telephone and, in some services, through text-based communication. ICPHAA recognises that online and telephone work, delivered competently and ethically, can greatly improve access for people facing barriers to in-person support, including distance, mobility, caring responsibilities and personal preference. It also brings specific ethical, clinical, legal and technical challenges.

This policy sets the standards members are expected to meet when working remotely, when using technology to communicate and keep records, when using social media, and when providing a physical space for clients. It applies the duties of confidentiality, competence and care in the ICPHAA Code of Conduct for Members to the settings in which members now work.

2. Scope

This policy applies to all ICPHAA members, in every membership category, who:

- provide therapy, support or supervision by video, telephone, email, messaging or any other remote means;
- use computers, phones, tablets, cloud services or software to communicate with clients or to hold client information;
- maintain a website, directory listing or social media presence connected with their professional work;
- see clients in person, whether in a clinic, shared premises, an organisation or their own home.

Members working within an organisation should also follow that organisation's IT, data protection and premises policies. Members who work with clients outside Ireland should also read the Cross-Border Practice Policy.

3. Suitability and consent for remote work

Before beginning online or telephone work, members make an informed assessment of whether it is suitable for the client, taking into account:

- the nature and severity of the presenting issues, and any known risk of harm to self or others;
- the client's access to, and confidence with, the technology;
- whether the client has a private, safe space from which to take part, free from being overheard or monitored by others;
- the client's age and, for younger clients, the involvement of parents or guardians;
- the availability of local crisis and support services where the client lives.

As part of informed consent, members explain how remote sessions will work, the platform to be used, how confidentiality and data are protected, what happens if the connection fails, and the limits of the support a member can provide to someone in crisis at a distance. Suitability is kept under review, and members should offer in-person work or a referral if remote work stops being appropriate.

4. Platforms and data protection

Members are responsible for the security of the tools they use. In particular:

- Client sessions take place only on secure, encrypted platforms that comply with the General Data Protection Regulation (GDPR) and the Data Protection Acts 1988–2018. Members check the provider's security and data processing terms and keep a record of that check.
- Members use professional accounts, not personal ones, for client work, and do not use open meeting links that others could join.
- Sessions are not recorded unless the client has given explicit, informed and recorded consent for a clear purpose, such as supervision or training, and the recording is stored securely and deleted when no longer needed.
- Members do not upload client information to artificial intelligence tools, transcription services or note-taking applications unless the client has given explicit informed consent and the service meets data protection requirements, including a suitable data processing agreement.
- Members take part in sessions from a private space where they cannot be overheard, and use headphones where others may be nearby.

5. Emergency and risk protocols

Every member who works remotely has a clear emergency protocol, agreed with the client at the start of the work. The protocol should include:

1. confirming the client's location at the start of each session, as they may not always be at the same address;
2. holding an emergency contact for the client, with their consent, and the details of local emergency and crisis services;
3. agreeing what will happen if the connection drops, for example the member will call the client's phone;
4. clear steps for contacting the emergency services where there is an imminent risk to life;
5. recording any incident, the actions taken and the reasons, and discussing it in supervision.

Risk assessment and safeguarding duties apply in full to remote work. The Safeguarding & Duty of Care Policy sets out how members respond to concerns about children and adults at risk.

6. Cybersecurity, communications and digital records

Protecting client information from unauthorised access is not merely a technical matter: it is an ethical obligation rooted in the duty of confidentiality. As a minimum, members:

- use strong, unique passwords for all professional accounts and devices, and a password manager where possible;
- turn on multi-factor authentication wherever it is available;
- keep operating systems, applications and security software up to date;
- lock devices when unattended and do not let others use devices that hold client information;
- encrypt client data stored on laptops, phones and portable drives;
- do not use public Wi-Fi for client sessions or to access client records unless a secure connection, such as a virtual private network (VPN), is in place;
- back up records securely and know how they would be recovered after loss or theft.

Email and messaging with clients should be kept to practical matters such as appointments, unless therapeutic work by text has been specifically agreed. Members tell clients how quickly they can expect a reply and that these channels are not monitored for emergencies. Digital records are subject to the same retention and secure destruction rules as paper records, as set out in the ICPHAA Code of Conduct for Members.

If a device is lost or stolen, or a member suspects that client data has been accessed without authority, they must act promptly in line with their obligations under data protection law, which may include notifying the Data Protection Commission and affected clients.

7. Social media and online boundaries

Social media can blur the line between professional and personal life and can compromise the therapeutic relationship through unintended or inappropriate contact. Members therefore:

- do not accept or send connection, friend or follow requests to or from current or former clients on personal accounts;
- keep any professional accounts clearly separate from personal accounts, and make sure professional content is accurate and consistent with the ICPHAA Code of Conduct for Members;
- do not search for information about clients online without a clear clinical or safeguarding reason, discussed in supervision and recorded;
- never post or discuss client material, even in disguised form, on social media or in online forums;
- describe their qualifications, membership category and services accurately, and do not describe ICPHAA membership as statutory registration;
- review their privacy settings and consider what clients might find about them online.

ICPHAA's own social media accounts are managed in line with the Association's values. Matters relating to complaints or disciplinary proceedings are never discussed on social media.

8. The physical practice environment

Whether working in a clinic, shared premises, an organisation or at home, members provide a setting that is private, safe and appropriate for therapeutic work.

- **Privacy.** Sessions cannot be overheard or interrupted, and clients are not seen by others any more than is unavoidable. Waiting arrangements protect clients' privacy.
- **Safety.** Rooms are safe and well maintained, with a clear exit, and members have a plan for managing risk, including lone working.
- **Accessibility.** Members consider the access needs of clients with disabilities and make reasonable adjustments in line with the Equal Status Acts 2000–2018, or refer to a suitable alternative.
- **Records.** Paper records are kept in locked storage, and client information is never left visible in shared spaces.
- **Home-based practice.** Members working from home keep the therapy space separate from family life, make sure household members cannot overhear sessions or access records, and consider the personal safety implications of clients knowing their home address.

9. Responsibilities and breaches

Members are responsible for choosing secure tools, assessing suitability for remote work, keeping emergency protocols in place, protecting client data, maintaining professional boundaries online and providing a safe, private practice space. Members should keep their digital skills up to date as part of their continuing professional development.

ICPHAA is responsible for providing guidance on request through the ICPHAA Registry, for protecting the personal data it holds with appropriate technical and organisational measures, for carrying out a data protection impact assessment where the law requires one before introducing new systems, and for keeping this policy under review.

A failure to meet the standards in this policy that puts client confidentiality, safety or welfare at risk is a breach of the ICPHAA Code of Conduct for Members and may be considered under the Complaints Procedures and, where relevant, the Fitness to Practise Policy and Disciplinary Procedures. Questions and concerns can be sent to the ICPHAA Registry at admin@icphaa.ie.

10. Monitoring and review

Technology and the law relating to it change quickly. The ICPHAA Board of Directors owns this policy and reviews it at least annually, or sooner where changes in law, regulation, technology or professional practice require it. The current version is available at www.icphaa.ie.

READ ALONGSIDE

- ICPHAA Code of Conduct for Members
- Confidentiality Policy
- Safeguarding & Duty of Care Policy
- Cross-Border Practice Policy
- Legal & Data Governance Policy
- Insurance & Liability Policy

DOCUMENT CONTROL

VERSION	DATE	CHANGE	APPROVED BY
1.0	9 November 2026	Reissued in the ICPHAA policy framework (replaces the former ICPA version).	ICPHAA Board of Directors

Support · Develop · Empower

ICPHAA
SUPPORT · DEVELOP · EMPOWER
Irish Counselling, Psychotherapy & Allied Healthcare Professionals Association