KEEPING YOU SAFE

On the following pages you'll find information about:

+ How we protect you and your privacy + confidentiality
+ How to stay safe during face-to-face, online and telephone appointments

If you would like more information, please read our Privacy Policy, available online or at our centres. Our reception team would be happy to provide a copy.

Relationships
AUSTRALIA · NSW

Relationships Australia NSW adheres to Australian Privacy Principles.

Your Personal Information

We need to collect some personal information when you become a client at Relationships Australia NSW. The information you provide will be used to create your client record, provide effective service, and help us contact you.

Privacy

We are committed to respecting your privacy. All personal information is handled in compliance with Australian privacy law. For more detail on how we collect, use and disclose personal information please read our Privacy Policy available on our website or in hard copy in our offices.

Using Your Information

Relationships Australia NSW will only use your personal information for the purpose for which it was gathered, and other lawful uses such as service management, monitoring service usage, clinical audit, or educational and training purposes. We and our partners may also use anonymous information in our professional publications and presentations.

De-identified Feedback to Funders

Most of our services are funded by State or Commonwealth Governments. As part of their funding, they may require us to provide them with general information about people using our services and whether those services are helpful. Funding bodies cannot access identifying details like your name within this general information.

Confidentiality

We are committed to protecting your confidentiality. All staff sign a Confidentiality Agreement and will only provide client details outside of the organisation when we are required by law, or authorised by law, to do so.

Limits to Confidentiality

State and Commonwealth legislation requires staff to notify the relevant authority if they reasonably believe that a person's health and safety, or that of the public, is at risk. This includes if there are safety concerns about children or young people. Confidentiality cannot be kept in some situations, such as the following:

- Staff may become concerned about your safety, the safety of your property, or about information following a major crime. If this happens, the staff member may have an ethical, professional or legal obligation to promote safety by informing appropriate parties.
- State laws require staff to notify a prescribed child welfare authority if they have reasonable grounds for suspecting a child has been abused or is at risk of being abused. Staff will follow the relevant State Government Information Sharing Guidelines to prevent harm to children's development.
- The Family Law Act 1975 (Cth) requires practitioners (such as family counsellors and family dispute resolution practitioners) to disclose client information if there have been any admissions, or reasonable grounds for suspecting, that a child has been abused or is at risk of being abused.
- For some services, practitioners may need to disclose client information to assist an Independent Children's Lawyer (ICL) appointed under the Family Law Act 1975 (Cth) to properly represent children's interest in family law court proceedings.

Information in Family Law Act 1975 (Cth) Programs

Some of our programs are covered under the Family Law Act 1975 (Cth) which provides specific protections preventing confidential client information from being

used as evidence in court proceedings (i.e. inadmissible information). It is important to know that not all client information in these programs is inadmissible, and we may still be required by law to disclose confidential information. Talk to your practitioner to find out if your program is covered by the Family Law Act 1975 (Cth).

Research and Surveys

De-identified data is used for research and evaluation purposes, including compiling statistics to guide us and our funders on how to improve our services. Surveys are sent out to clients at regular intervals to hear about their experience with us. You may choose to opt out of these communications at any time.

Confidentiality in Appointments - No Recordings

All meetings and appointments are private and must not be recorded. This includes not recording on the device you are using or by another recording or listening device. You must not allow another person to record the appointment. Any recordings made may be an offence under the Surveillance Devices Act 2007 (NSW) and can result in penalties. If you are unsure of your legal obligations and rights it is recommended that you seek independent legal advice.

Keeping Online and Phone Appointments Secure

Relationships Australia NSW uses industry-standard devices and trusted software for your appointments. We strongly recommend that you receive appointments on secure hardware by consulting the eSafety Commissioner and Techsafety websites about your security and privacy online. We cannot guarantee the security of any service provided by a third party.

Safety During Appointments

To keep you (and your family's) physical location private, it is essential to take the following precautions during the session.

Complete a thorough scan of your background and make sure there is nothing on camera that can identify your location, such as:

- anything that shows the front of your house
- anything that shows an identifiable landmark on your street
- anything that shows where your child attends school such as a uniform or school bag
- documents containing your address
- your work uniform, ID badge or work documents
- photographs or monitor screens showing any of the above
- any distinctive sounds.

Avoid moving around with your device during the meeting.

Risks to Consider When Using Video in Appointments

We will only use video-conference platforms that operate end-to-end encryption using the Advanced Encryption Standard (AES). However, even these platforms may have unknown security vulnerabilities. If we discover such vulnerabilities, we will immediately fix them or switch to another platform. Whilst highly unlikely, examples of the risks in using video in appointments include:

- Finding someone's location by discovering their IP address (i.e. where your computer is connected). This risk is low, and your risk may be minimised by changing IP address by rebooting your modem (which may pick up another IP address from the pool of IP addresses that your Internet Service Provider has).
- Someone may 'hack' and overhear or record the conversation if a device has been compromised by a virus that detects activity on that device. Your risk of this may be minimised by using an up-to-date anti-virus program and operating systems.
- Incurring cost from receiving video appointments. You can minimise this risk by checking if your data plan can cover approximately 1GB of data per hour of appointments or by using an unlimited NBN or broadband plan.