Office of the Migration Agents Registration Authority
Practice guide for registered migration agents

Client confidentiality – storing and transmitting client information

The *Migration (Migration Agents Code of Conduct) Regulations 2021* (the Code) sets out that a Registered Migration Agent (RMA) has a duty of confidentiality to their clients. Section 35 of the Code requires that, except as required by law, an RMA must not disclose, or allow to be disclosed, to a third person any personal information relating to a client or former client or their affairs without the client's written consent.

Section 53 of the Code sets out the duty of an RMA to keep documents securely. *A migration agent must ensure that any documents belonging, or relating, to a client or former client of the agent that are in possession of the agent, or member of the agent's business are kept securely.*

Registered migration agents should take reasonable practical steps to adequately safeguard their client's personal information. This includes where that information is stored electronically.

Electronic storage of client documents encompasses the security of storage of electronic documents in a variety of media and in a range of locations - for example, the computer's hard drive, the server, on a tablet, smartphone or on a portable memory device such as an SD card or USB stick.

An RMA's compliance with their obligations is potentially at risk where the transmittal and storage of client information is not accompanied by adequate safeguards.

Email security

Emails form much of the communications an organisation has internally and with business partners and customers. These electronic records may contain information relating to visa applications, conversations with clients and information provided to the Department of Home Affairs.

It is vital that these records are transmitted securely. Agents should:

- ensure wireless connections are secure
- use reliable software to prevent viruses
- be wary of opening attachments
- ensure emails are backed up regularly
- consider encryption for highly sensitive information
- ensure emails are sent to the correct recipient
- consider using a legal disclaimer at the top of any email that contains private data.

Tips for storing client information

Ensure any third party that hosts client data is reputable

Risk: Data compromised when control is lost - confidential client information falls into the wrong hands.

- Check the third party's ownership and whether owned or controlled by a reputable company.
- Identify where geographically the data will be stored.
- Find out who will have access to the data and how access will be controlled.
- Find out what happens when data is compromised and whether you will be notified in a timely manner.
- Consider whether it is really cost effective to have data stored offsite, having regard to all the risks.

Carefully manage portable storage devices

Risk: Potable storage device is lost or stolen - confidential client information falls into the wrong hands.

- Avoid use of portable storage devices where possible – they are easily lost and prone to theft.
- Use password protection.
- Change your password frequently.
- Encrypt data on discs, USB flash drives, SD cards and the like.
- Lock portable storage devices away securely.

Protect and secure laptops

Risk: Laptop damaged, lost or stolen - confidential client information falls into the wrong hands.

- Use a reliable antivirus program and a personal firewall and keep them regularly updated.
- Backup the information on your laptop to a secure device or site as often as possible.
- Don't store unnecessary confidential information on a laptop's hard drive.
- Never leave access numbers, passwords or security devices in your laptop case.
- Where possible, carry your laptop with you and always keep a close eye on it — pay careful attention when going through airport security and avoid leaving your laptop in a parked car.

Keep hard copies of client information secure

Risk: Hard copies duplicated, lost or stolen - confidential client information falls into the wrong hands.

- Employ a 'clear desk' policy — hard copies containing a client's personal or sensitive details should be filed and locked away securely at the end of each day.
- Keep paper files in locked filing cabinets unless actively working on them.
- Make sure filing cabinets are locked at night or during the day if the office is unattended for an extended time.
- Use a secure print function when printing in an open office environment.
- File printed material promptly and lock client files away when not in use.
- Use a shredder rather than disposing of unwanted information in normal waste.
- Keep a register of significant documents held (such as passports and original client documents).