LAURA BYERS

WILLS | TRUSTS | POWERS OF ATTORNEY

# Cyber Security Policy

I offer legal advice in relation to the provision of wills, powers of attorney and other related transactions. In this capacity, I make use of the following systems:

- Clio – client management system
- Arken – will drafting software
- Microsoft Office 365 Professional (includes One Drive)

**Policy brief & purpose**

My cyber security policy outlines my guidelines and provisions for preserving the security of client and other data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage, client exposure and possible reputational damage.

For this reason, I have implemented a number of security measures. I have also prepared instructions that may help mitigate security risks. I have outlined both provisions in this policy.

**Scope**

This policy applies to me and to anyone who has permanent or temporary access to my systems and hardware.

**Policy elements**

**Confidential data**

Confidential data is secret and valuable. Common examples are:

- Client financial information
- Client personal information
- Personal information of relatives and friends of the client named as executors, trustees, guardians, beneficiaries etc
- Client lists (existing and prospective)

I am obliged to protect this data. In this policy, I will set out how I will avoid security breaches and how any contractors or other third parties instructed by me will ensure that I avoid security breaches.

**Protect personal and business devices**

When I use my digital devices to access work emails or client management and/or drafting systems ("CMS"), I am introducing security risk to client and other data. I keep both my personal and business computer, tablet and mobile phone secure by ensuring that I:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure that I do not leave my devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into my client management systems and email accounts and through secure and private networks only.

I also avoid accessing internal systems and accounts from other people's devices with access to client data or lending my own devices to others.

**Keep emails safe**

Emails often host scams and malicious software. To avoid virus infection or data theft, I:

- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Avoid opening emails with clickbait titles (e.g. offering prizes, advice).
- Check the email/ names of people I receive messages from to ensure that they are legitimate.
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

**Manage passwords properly**

Password leaks are dangerous as they can compromise my entire infrastructure. Not only should passwords be secure so that they will not easily be hacked, but they should also remain secret. For this reason, I:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be guessed easily (e.g. birthdays).
- Remember passwords instead of writing them down or only retaining a secure digital record.
- Exchange credentials only when absolutely necessary. When exchanging them in person is not possible, I would only ever exchange details by phone instead of email, and only if I personally recognise the person that I am talking to.
- Change my passwords every two months.

**Transfer data securely**

Transferring data introduces security risk. I will:

- Avoid transferring sensitive data (e.g. client/beneficiary information) to other devices or accounts unless absolutely necessary. If mass transfer of such data is needed, I will utilise the services of my IT contractor.
- Share confidential data through the communication services of my CMS or through Outlook and not over public Wi-Fi.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.

- Report scams, privacy breaches and hacking attempts.

My IT contractor needs to know about scams, breaches and malware so they can better protect my infrastructure. For this reason, I will report perceived attacks, suspicious emails or phishing attempts as soon as possible to our them and request that they investigate promptly, resolve the issue and any necessary changes will be implemented.

**Additional measures**

To reduce the likelihood of security breaches, I also:

- Turn off my screen and lock their devices when leaving my desk.
- Lock/report any stolen or damaged equipment as soon as possible.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in my systems to my IT contractor.
- Refrain from downloading suspicious, unauthorised or illegal software on my equipment.
- Avoid accessing suspicious websites.

In conjunction with my IT contractor, I will:

- Install firewalls, anti-malware software and access authentication systems.
- Stay abreast of new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.

I will have all physical and digital shields to protect information.

**Working remotely**

When working remotely, I will follow this policy's instructions also; following all data encryption, protection standards and settings, and ensuring that my private network is secure.

**Take security seriously**

Everyone, from my clients to my contractors, should feel that their data is safe. The only way to gain their trust is to protect my systems and databases proactively, by being vigilant and keeping cyber security in the top of my mind.

**Specifics**

**Laptop** – pin protected, and hard drive fully encrypted in case of loss or theft.

**Clio** – Cloud-based, auto-software updates, recommended by the Law Society, secure client access, links securely to Arken

**Arken** – Cloud-based, auto-software updates, links securely to Clio, commitment to maintaining the highest operational standards in systems and processes to protect personal data. Multiple layers of security controls including physical and network security, firewalls and intrusion protection systems. Arken engages industry leading suppliers to leverage their expertise, experience, global threat and intelligence to protect its systems. It uses the latest industry standard SSL and TLS 1.3 (Transport Security Layer) with HSTS (HTTP Strict Transport Security) for enhanced security and all data is encrypted in transit. Arken uses enterprise-grade hosting facilities that are PCI and ISO accredited and employs robust physical security controls to prevent physical access to the service and redundant power, air-conditioning and

communications. Controls include 24/7/365 monitoring and surveillance, on-site security staff and regular on-going security audits. User data is held in accordance with Arken's Privacy Policy, only authorised Arken personnel have access to data which is strictly limited to essential personnel only and only from Arken equipment and Arken continuously monitors event logs, notifications and alerts from all systems to identify and manage threats.

**Microsoft Office 365 Professional** – this includes many in-built security features including multi-factor authentication, adding a layer of protection to the log in process, mobile device management, Advanced Threat Protection to counter ransomware which is spread almost entirely through malicious links and attachments in emails.



For information on how I handle your personal data, please see my privacy notice on my website. This letter is intended for the addressee only. This includes any attachments. Its unauthorised use, further processing, storage or copying is not allowed. If you are not the intended recipient, please let the sender know and then destroy all copies.

Authorised and regulated by the Solicitors Regulation Authority (SRA number 165280)