Taking Data Security Seriously
A common misconception related to cloud computing and hosted IT is that the operational benefits on offer are accessed at the expense of data security. The reality is that increased data security is another potential benefit of a DPSCloud hosted IT solution.

DPS Software understand and respect the importance of data security to law firms operating under today’s business and legal sector-specific regulations. Our commitment to safeguarding the data our hosted clients place under our guardianship is evident in our accreditation to the ISO/IEC 27001:2005 international information security management standard and the operating policies and procedures this entails.

Your firm’s database is your property and contains confidential information on your clients. Hosting this information away from your premises, as mentioned before, can lead to concerns over security. For this reason as part of the hosting contract, DPS enter into a Non Disclosure Agreement (NDA) with your firm to offer you the protection you require for your data.

Ownership of the information stored by us for you remains, with your firm at all times. Hosting services include the backing up of your information to both an off-site DR facility and backup tapes, as well as the storage of backup tapes at our premises. The contents of these tapes remain your property and will be forwarded to your practice when requested.

In practice the information security management system (ISMS) in place at DPS would be prohibitively expensive and extremely labour intensive to implement at law firms who increasingly cannot afford distractions from their focus on legal work. Keeping servers and data on site may
well give law firms a feeling of security but if they lack the proper infrastructure, management systems and expertise then this feeling is essentially false.

In addition to the NDA, our service level agreement covers all eventualities such as disasters and unforeseen business conditions.

Whether your data is hosted or not at some stage a software vendor will need access to your information. They will often take copies of your information for investigation or other purposes. DPS enters into the NDA and service agreement whether hosting is provided or not, as it is highly advisable when any company has any access to your information.

Sample agreements are available for inspection at the contract stage of a negotiation as is access to the manuals, policies, procedures and operations/admin documents which make up our ISMS.

On the following page you can find a summary of some of the key measures DPS employs to ensure your data is kept secure when under our guardianship...
DPSCLOUD SECURITY SUMMARY:

- DPS has multiple high-capacity Internet lines coming into the building from different exchanges and ISPs. They are aggregated via link balancing hardware. This also provides a degree of resilience in the case of line failure as the link balancers also act as a DNS name server with a short TTL. The link balancers are clustered.

- DPS has a dual firewall / DMZ configuration. The DMZ contains all the web servers and any edge of network equipment that faces the internet. Critical servers are clustered on virtual servers which will provide a level of hardware redundancy. The firewalls are set up in a High Availability configuration.

- Behind the firewalls the servers are separated by VLANS for extra security above the domain level security.

- The servers for Citrix, SQL and exchange are clustered on blade servers. The blades are monitored through the carcass. We have an iSCSI SAN network which stores the VMs for the blades. This allows us to move the VM processes between the blades gracefully.

- All our mail is scanned for Spam and Viruses by hardware within the DMZ. This is before any emails reach the exchange servers thus protecting the servers from overload and Rate attacks. All web access is monitored and checked for malicious code. This again is done within the DMZ.

- The version of Citrix used is SSL certificated 256-bit encrypted, the highest level of encryption available without having to report its use (and provide encryption codes) to government agencies. This is a protocol which creates a secure connection between a client and the server over which to send information.