Queensland Law Society

QLS Innovation Committee – Hybrid work taskforce

Considerations for IT Challenges

Cyber Security

- ☐ How are your staff accessing the network? Has this been assessed from a Cyber Security perspective?
- ☐ Does remote access from your Staff from home pose any greater risk to your Cyber Security? If so, what steps are necessary?
- ☐ Do you have processes and the ability to deal with a cyber incident that happens to a staff member's computer equipment at their home or other remote site?
- ☐ Do you have adequate insurance in place which will respond to cyber attacks and other cyber issues?[1]
- ☐ Are your staff trained in cyber security and cyber risks?

Refer to the QLS Cyber Security guide for more information **qls.com.au/Content-Collections/Guides/Cybersecurity-risk-assessment-tool-for-small-law-f**

Many of the issues raised are covered by QLS guides. See **qls.com.au/Practising-law-in-Qld/Resources/Cybersecurity**

Equipment Inventory

- ☐ What IT equipment do you permit your staff to take home? Is this equipment required to be bought back to the office on days when they are working from the office?
- ☐ Do you have an inventory of IT equipment that your staff are required to record when taking equipment home?
- ☐ What is your process for taking care of equipment when it is not in the office?
- ☐ What is your lost property process?

Network Connections and Outages

- ☐ Do you have minimum requirements for network connections for your people from home to ensure they have adequate speed for use of technology? Are your staff connecting via a trusted network?
- ☐ Do your staff have internet equipment at home that allows an internet connection sufficient to do their work (i.e. that is not affected by other family members using the internet connection at the same time)?
- ☐ What is your process or procedure if their "internet is down" or "slow" on a work from home day – are they to come into the office?

[1] QLS has up to $50,000 cover in place for "Member Firms". To check eligibility and terms consider **qls.com.au/Services/Business-Services/Cyber-Essentials-Insurance**

Always “on”

- [ ] What is your process for ensuring that your staff are not “always on” if they have IT equipment (such as laptops) set up at home

Communication & Collaboration between staff

- [ ] What options do you have for staff to “speak” to each other during the day? Are they able to collaborate using technology throughout the day?
- [ ] Do your IT platforms allow for Junior staff to connect with colleagues – peers and senior staff adequately?

IT Strategy

- [ ] Do you have an IT strategy which is relevant to the needs of your practice and your clients?
- [ ] Do you have an IT procurement policy relating to things such as the portability of IT resources, consistency of resources and compatibility of hardware devices?
- [ ] What level of IT equipment do you require your staff to have at home (if it is not supplied by your firm)?
- [ ] Do you have appropriate IT resources that allow all your staff to work from home, and do everything that they would usually do if they were in the office?
- [ ] Are your IT tasks properly resourced? Even if you have an internal IT team, some matters may be outside their capabilities or experience.