Cyber Security Good Practice Guide

It is important for members to consider how they are protecting their client data and safeguarding their practice against cyber threats. This guide outlines some practical steps that can be taken to strengthen your cyber security.

1. Use of Cyber Security Resources

Take advantage of official guidance and reputable resources on cyber security. There are several Government backed initiatives which provide further support for businesses, including:

- Cyber Aware – a cross government initiative aimed at promoting secure online behaviours for small businesses and individuals.

- Free online training courses for businesses and their staff.

- The National Cyber Security Centre offers a wide range of guides on all areas of cyber security.

2. Assign Responsibilities

Decide who in your practice is responsible for overseeing cyber security matters. Provide that person with the authority and resources to monitor risk and act quickly if an incident occurs.

3. Incident Response

Develop a clear plan for dealing with cyber incidents. This could include how to contain the problem, the method for communicating the issue to your clients, and any regulatory and legal reporting obligations that may arise because of the incident.

4. Basic Protections

Keep all software and operating systems fully up to date. Install anti-virus and anti-malware tools. Back up data regularly and test that the back ups can be restored when needed.

5. Password and Access

Use strong, unique passwords and enable multi-factor authentication where possible. Limit user access to only information necessary for their role and review those permissions periodically. Put procedures in places to track and remotely wipe lost or stolen devices. Prohibit the use of insecure WiFi hotspots.

6. Awareness and Training

Provide regular staff training on recognising common cyber threats such as phishing emails. Encourage prompt reporting of anything suspicious and make sure everyone knows how to escalate concerns. Keep training materials up to date to reflect new and emerging threats.

7. Third-Party Providers

Ensure software suppliers and cloud providers have robust security in place. Understand where your data is stored and how it is being protected.

8. Cyber Insurance

Consider whether cyber insurance is appropriate for your practice. Policies can help cover the cost of data breaches, ransomware attacks and business interruption. Insurers often provide practical support and helplines. As with all insurance, policies vary greatly, ensure you examine the scope of cover and any exclusions carefully.