Cybersecurity Checklist

RMS

- [ ] 1 **Protect your database by choosing a complex password that is unique** (i.e. not used for any other applications) and contains 10+ characters. Store in a secure password manager.

- [ ] 2 **Add an extra layer of defence by enabling two-factor authentication.** This additional step will ask you to confirm your identity via your trusted device.

- [ ] 3 **Regularly review users on shared databases** and check your system access reports to confirm all recent logins are from genuine users that you recognise.

- [ ] 4 **Complete cybersecurity training.** If your place of work doesn't provide training, raise it with a manager. Alternatively, there are free online courses available to refresh your knowledge.

- [ ] 5 **Identify, report and block any scam or phishing emails.** Review domains and don't click any suspicious links.

- [ ] 6 **Update your software as and when required.** Back up important files in case of a data breach so that you can retain details and take appropriate action, should a breach occur.

- [ ] 7 **Review your security policy** to stay up to date with company procedures and security protocols.

- [ ] 8 **Take the pledge.** Sign here to confirm that you have read the above, taken action where necessary and are committed to taking the necessary steps to protect your database. _____

PRINT OFF THIS CHECKLIST AND MAKE SURE ALL BOXES ARE TICKED FOR MAXIMUM SECURITY PROTECTION.