Mansfield College Information Security
Policy Guidance Notes

1 INTRODUCTION

These notes are intended to offer specific guidance to interpreting sections of the Mansfield College Information Security Policy. They highlight key areas of the policy and clarify their significance as they apply to different members of the College.

Note that the entire policy still applies to all members, irrespective of whether specific guidance notes have been given.

2 STUDENTS

9.3: As students have no access to confidential information this section is largely irrelevant.

9.5: Please note the rules for connection to the internet under 3a mandate the use of both anti-virus software (preferably Sophos) and your computer’s built-in firewall.

9.6: Please note that you are required to set a passcode on any device with network access.

9.7: As students have no access to College information or systems this section is largely irrelevant.

9.8: Students are not entitled to College software under our license agreements.

9.9: As students have no access to College data this section is largely irrelevant.

9.10/9.11/9.12: These cover College back office systems and are largely irrelevant.

3 FELLOWS

9.3: Teaching or research materials do not count as confidential information unless covered elsewhere (e.g. medical research data).

9.5: Please note the rules for connection to the internet under 3a mandate the use of both anti-virus software (preferably Sophos) and your computer’s built-in firewall. If you have access to important or confidential College data, please exercise judgment before accessing or copying it.

9.6: Please note that you are required to set a passcode on any device with network access.

9.7: As most Fellows have no access to College information or systems this section is largely irrelevant.

9.8: Only College owned desktops are entitled to College software under our license agreements.

9.9: Teaching or research data is explicitly exempt from these rules unless by other agreement.

9.10/9.11/9.12: These cover College back office systems and are largely irrelevant.
4 Administrative Staff

9.5: Note particularly that you are not permitted to use your own computing equipment for College purposes without approval from the IT Manager.

9.6: You should not be using mobile computing for work purposes without discussing your requirements with the IT Manager. Also, note that you are required to set a passcode on any device with network access (such as your mobile phone).

9.9: Note particularly that you may not store copyrighted material on College systems, and that we reserve the right to access any system you are provided with in certain exceptional circumstances.

9.10/9.11/9.12: These cover College back office systems and are largely irrelevant.