Guidance on Remote Working

This guidance: -

- is intended for all staff who work away from the University on an occasional or regular basis.
- applies to anyone undertaking any University work away from the University premises.
- applies to recorded information in all formats: paper, electronic data, correspondence, and, e-mail.

Do:

- Remember that as all work-related documents are University records, and as such fall within the scope of Freedom of Information and Data Protection, you should follow the IMPS guidance below.
- Work directly from the appropriate University server via a secure Virtual Private Network connection.
- Save any electronic documents produced at home on to University network storage.
- Take copies of paper files or electronic documents home rather than originals, unless there is no alternative.
- If you have to take original files home, ensure that this is recorded in your department.
- Make use of security features such as password protection & data encryption.
- Take all reasonable steps to maintain security of and prevent loss or damage to any data and/or records taken away from the University.
- Use your University e-mail account for University work and your personal email account for personal use only; avoid mixing the two.
- Encrypt memory sticks that hold University information.
- Keep your computer system and applications virus-protected and up to date.

Do Not:

- Use your home computer to store University information.
- Remove a paper file from the University unless it can be stored securely.
- Leave paper or electronic files where they could be accidentally viewed by others, including family members.
- Use a personal e-mail account for University business
- Leave University data or electronic media in unattended vehicles, even if locked in the boot.

For further explanation see additional 'Working from Home' information at: -
http://www.reading.ac.uk/internal/imps/DataProtection/imps-d-p-guidelines.aspx