

# ST AUGUSTINE RESEARCH & REFERENCE SERVICES (STARRS)

## Rules of conduct

All users are expected to respect the policies governing the use of the Main Library's computing facilities. Rules of conduct to be observed in STARRS are as follows:

- Only users with a valid ID are permitted access to STARRS. Users are required to show their current University ID upon request, to any member of staff at any time.
- Users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able access their account. Under no conditions should users provide their user ID and password to another person.
- Users should never store any files documents on the desktop or C: drive of any PC. These are wiped clean on a daily basis. Store all files on an external storage device (thumb drive/USB flash drive).
- Users are strictly prohibited from using cellular phones for any purpose in STARRS. All phones must therefore be switched off.
- No loitering is permitted in STARRS. Due to limited resources there are no provisions for group work, therefore only one user is allowed at a terminal.
- Users are to observe silence at all times. Loud sounds either from the computers or from headsets are disruptive.
- Under no circumstances are users to consume food or drink in STARRS at any time of the day or night.
- Games and other entertainment enjoyed on lab equipment always have the lowest priority. During periods of peak demand, PCs may be re-deployed to students who require them for academic pursuits.
- Users are not to disrupt the computer systems by tampering with hardware and/or software configurations, or to destroy data by spreading, accessing or writing computer viruses, or by other means.
- Users are not to attempt to gain unauthorised access to any other computer system through STARRS or go beyond their authorised access. This includes attempting to log in through another person's account or access another person's files.
- Users will not use STARRS to engage in criminal activity including but not limited to threatening the safety of other persons, transmitting fraudulent, defamatory, harassing, obscene, or threatening messages, or engaging in any communications prohibited by law.

**Failure to abide by these regulations may result in the withdrawal of network privileges.**

Dr Hannah Francis  
Head User Services Division