Policy for remote connection to end user desktops

Name of policy, procedure or regulation	Policy for remote connection to end user desktops
Purpose of policy, procedure or regulation	To detail actions staff should and should not take when initiating a remote connection an end-users computer
Who formally approved this policy, procedure or regulation?	Information Technology Management Board
Who has responsibility for its update?	Information Services

To whom does this policy, procedure or regulation apply?

All University staff

a) Date of approval	4th Nov 2014	**b) Proposed date of review**	Annual

1. Introduction/Rationale

In order to effectively support users, IT support staff use a range of remote support tools that enable manipulation of files, system settings, control of keyboard and mouse, and remote viewing of the screen. This document outlines the scope of any authorised remote connection, and the procedures that staff should follow when initiating a remote connection.

2. Remote Connection Policy

It is important that staff are made in advance aware of any remote connection to their machine and what such a connection means to them in terms of the privacy of and confidentiality of their data. To facilitate this

Support staff must:

- Contact the user prior to any of the following actions to gain their explicit consent:
  - viewing the content of the user's screen
  - opening any e-mail software (Outlook, etc.) or viewing the content of any message
  - viewing, modifying, moving, copying, or deleting any document belonging to the user (e.g. Word, Excel, PowerPoint files, etc.)
- Inform the user at all stages of what actions are being taken and any implications for the user or the privacy of their files or data

Support staff may:

- Delete files from student lab machines, GTR machines or other public machines as part of system management processes
- Connect to a machine using in a separate session (screen) than that of the user, for support purposes

- Remotely open, modify, copy or delete system configuration files for support purposes
- Delete /clean viruses or Trojan files to ensure the stability of the network.

Under special circumstances, the Director of Information Services, Head of Personnel, Executive, or appropriate Directors of Service or Deans of Faculty may authorise an investigation that explicitly allows use of remote tools to view a user's files, screen, or email. In such cases permission will be given to IT support staff in advance.

The University views unauthorised remote access to computers as a serious disciplinary offence. Any breach of these regulations shall be dealt with in accordance with the disciplinary procedures of the University applicable to the person concerned. Authorisation to use remote access tools may be withdrawn immediately, by a decision of the Director of Information Services, or the appropriate Dean of Faculty or Director of Service.