Network Security Policy

15/01/2014
Paul Vincent – Head of Technology and Media

Revised:

12/09/2015
18/10/2017

The Open College of the Arts has a responsibility to maintain the security and integrity of its on-site and remote technology. Therefore, the following policy and the protocols it contains must be followed by all staff, and related to all contractors and visitors to the college site.

- Any external non-OCA procured, or vetted, devices brought into the college must not be connected directly to the college network via Ethernet. Personal devices may be connected to the college's UCA Guest WiFi network.
- No external storage devices are to be attached to college computer equipment without prior approval of the Head of Technology and Media, or a member of their team. External storage devices must only be attached to computers which have been disconnected from the wired and WiFi network, and must be subjected to a virus check prior to their contents being downloaded.
- All college staff, whether on or off site, must use 2-Step/2Factor Authentication on their college Email accounts at all times. Failure to comply will result in the college's disciplinary procedures being applied.
- It is the duty of college staff to immediately notify all other staff of any suspicious, deceptive or malicious emails being received or circulated more widely.
- It is the duty of college staff to immediately inform a member of the technology and media team when a college-provided email account is suspected of having been hacked.
- Any files containing personal or sensitive student data must be encrypted before being taken off-site on a physical device.
- No account passwords belonging to individual members of staff are to be shared with any other individuals unless authorised to do so by a line manager.
- Anti-virus software must be installed and kept up to date on all college computer equipment.
- Extreme caution must be applied when using public WiFi for college business through college-provided equipment or personal devices. No sensitive stakeholder data is to be accessed through public WiFi under any circumstances.
- Any suspected breach of the college's on-site network security must be immediately reported to the OCA Head of Technology and Media, and in their absence, the OCA Principal or an OCA Director, for the issue to be escalated to the appropriate UCA contact.

8. Document Control

Document Name	Network Security Policy
Document Number/Version	POL-IT-002/3
Document Author	Paul Vincent, Head of Technology and Media
Approving Body	OCA Executive Group
Signature of Approval	
Date of Approval	08/05/18
Date Effective from	08/05/18
Review Date	01/10/18
Document this supersedes	N/A
Is this document for public access	Yes