Open College of the Arts

Network Security Policy

Document History

Version no	Status	Policy Owner	Approved by	Date of approval
1	Superseded	Paul Vincent	SMT	15/01/2014
2	Superseded	Paul Vincent	SMT	12/09/2015
3	Superseded by UCA	Paul Vincent	SMT	01/09/2018
4	Approved	Paul Vincent	OMG (chairs action)	01/11/2021
5.	Approved	Paul Vincent	Principal	09/12/2022

Commented [1]: Added section on non-compliance.

1. Overview

The Open College of the Arts has a responsibility to maintain the security and integrity of its on-site and remote technologies.

2. Purpose

The purpose of this Network Security policy is to ensure that all digital tools and systems employed for use by college stakeholders are protected to a level which minimises the impact of security-related events or incidents.
This policy, when applied, will provide the following protections for college assets, data and systems:

- Confidentiality: to ensure that the risk of data breaches is minimised.
- Integrity: to ensure that stored and transferred data is accurate and not corrupt

- Availability: to ensure that required data, services and assets are available to staff and other college stakeholders when required.
- Compliance: to ensure that the college's systems, data and processes meet the requirements of EU/UK legislation and industry expectations.

3. Scope

3.1 This policy applies to all staff, whether working off-site or at the college site at DMC02 in Barnsley. The policy must also be followed by any contractors of the college as well as any non-contracted visitors brought into the college where they are being provided with access to the college's networks or systems.

3.2 This policy covers all on-site networks, including WiFi Access Points (APs), Ethernet connections, as well as the use of public or home-based networks.

4. Network access

4.1 The college's on-site network can be accessed directly via ethernet or through the 'OCA' access point.

4.2 Access Point passwords must not be disclosed to non-staff members. Visitors must use the DMC02 public WiFi network.

4.3 Home network access must be secured by staff members using a highly secure password in line with the college's *Password and Authentication policy (internal use only)*. This is a prerequisite for staff to work from home.

4.4 Use of public WiFi must not be used to access any personal data relating to:

- Students
- Employees
- Contractors
- Secure and sensitive environments e.g. private servers, payment gateways, banking portals.

4.5 For security and network maintenance purposes, authorised individuals within OCA may monitor equipment, systems and network traffic at any time.

4.6 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.

4.7 Any suspected breach of the college's on-site network security must be immediately reported to the ICT team, the Head of Technology Enhanced Learning, and in their absence, the OCA Principal or another Director, for the issue to be escalated to an appropriate contact.

5. Device security & BYOD policy

5.1 Any external non-OCA procured, or vetted, devices brought into the college must not be connected directly to the college network via Ethernet or WiFi. Personal devices may instead be connected to the building's Guest WiFi network.

5.2 No external storage devices are to be attached to college computer equipment without prior approval of the Head of TEL, or an authorised member of ICT staff. 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.

5.3 All college staff must use 2-Step/2Factor Authentication on their college Email accounts at all times to ensure the data security of services being connected to.

5.4 Any files containing personal or sensitive student data must be encrypted and checked-out before being taken off-site on a physical device.

5.5 Antivirus software must be installed and kept up to date on all college computer equipment.

5.6 All OCA devices must be encrypted and installed with Antivirus software (Sophos) prior to their being provisioned to staff.

6. Communications security

6.1 College email technologies and the communications issued by them through the oca.ac.uk domain are secured and verified through use of SPF, DKIM and DMARC security measures to reduce the risk of successful phishing attempts. All Email sent by college staff, students, long-term contractors and tutors must be sent from college-provided email accounts.

6.2 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.

6.3 It is the duty of college staff to immediately inform a member of the ICT team when a college-provided email account is suspected of having been compromised.

6.4 It is the responsibility of staff in receipt of Google Workspace Incident Reports to investigate the report and escalate accordingly.

6.5 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.

7. Policy Compliance

7.1 Compliance Measurement

The ICT and/or TEL team will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

7.2 Exceptions

Any exception to the policy must be approved by the ICT and/or TEL Team in advance.

7.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.