ual:

# IT NETWORK AND ACCEPTABLE USE

## FOR STUDENTS

Inform users of their responsibilities for the protection of the University network and their own devices.

# Content

## SUMMARY



## POLICY



## APPENDIX

# Summary

## INTRODUCTION

Information Technology (IT) services are provided to University of the Arts London (UAL) students to support the teaching, learning, research and administrative activities of the University and are critical to the success of the University's mission, operations and business. However, the use of these facilities carries its own risks and the University wishes to make students aware of these risks and the steps that can be taken to alleviate them.

The data held within the University's IT systems and network forms part of its critical information assets. As a user of University provided IT services you are required to keep University information and data secure. You are also required to assist and support the University in carrying out its legal and operational obligations with regard to University data and information stored on its own systems.

This policy relates to the acceptable use of all IT services that are owned by, hosted and/or administered by the University. This includes:

- computer equipment, email and the internet
- connections made to external networks through the University network

- telephones, voicemail, smartphones, laptops, desktops, tablets
- fax machines, copiers and scanners

It outlines the standards we require users of these systems to observe and the action we will take in respect of breaches of these standards

This policy applies to anyone using the University's IT services ('Users'). This includes:

- students using either personal or University provided equipment which is connected locally or remotely to the University network
- visitors using University IT services
- students from other institutions logging on using Eduroam

In addition to this policy you must also abide by any regulations and policies applicable to other organisations whose services you access, such as JANET, Eduserv and JISC. When using services, you are subject to both the regulations of UAL and the institution where you are accessing IT services. (See Appendix A).

# WHO SHOULD READ THIS POLICY?

Students will be directed to this policy during their enrolment each year. This policy will be placed on the University website and/or Intranet. Changes to this policy may be communicated via email at the time of change.

# UNIVERSITY OF THE ARTS LONDON

The University is defined as the sites and physical locations which comprise the Colleges across London and University Services as follows:

- University Services at Holborn, Kings Cross and Elephant & Castle
- Camberwell College of Arts
- Chelsea College of Arts
- Wimbledon College of Arts
- Central Saint Martins
- London College of Communication
- London College of Fashion
- Academic Enterprise and associated entities
- UAL Halls of Residence

# THIS POLICY HAS BEEN ESTABLISHED TO:

Provide guidelines for the acceptable use of the University's computing and networking resources by students of the University, including the personal use of these services.

Inform users of their responsibilities for the protection of the University information, IT Services and their own devices.

Provide guidance which mitigates against information security risks, losses and threats arising from virus attacks and compromises of network systems and devices.

# DOS & DONTS

**Do** take care when accessing material that could reasonably be considered, by others, to be offensive, obscene, indecent or similar. In particular do not attempt to access content that is illegal or poses a security risk to IT services. The University reserves the right to monitor and block access to content that is considered illegal or poses a security risk to University IT Systems.

**Do** report, as soon as possible, any loss, theft or damage of University owned IT equipment

**Do** ensure you look after your own data

**Do** take care when using removable data storage such as USB sticks or into cloud-based storage devices such as Google Apps and

Dropbox. Students should make use of their University OneDrive account for this purpose. Although these services offer convenience and simplicity there are risks to their use which should be considered to eliminate the risk of data loss or unauthorised access

**Do** comply with copyright laws when using material such as images, text, music, film and software

**Don't** share your network password with anyone

**Don't** attempt to access material that is either illegal or could pose a security/malware risk to the University

**Don't** publicly disclose, in any way, any information about the security measures used to protect the University's information and IT networks

**Don't** install, use or distribute software on University owned devices unless the University is legally entitled to use the software for legitimate University purposes

**Don't** send emails which could be interpreted by others as being abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory

**Don't** attempt to circumvent or disable UAL IT services and devices configurations, or use utilities, techniques and devices to gain visibility of, corrupt, or impersonate UAL IT services, configurations and architectures, for any purpose

**Don't** connect unauthorised equipment to the UAL network

# Policy

## NETWORK USER IDS AND PASSWORDS

Under no circumstances should you share your network password with any other person.

## ACCESS TO OFFENSIVE MATERIAL

It is recognised that students in the course of their study, campaigning or research may have a legitimate requirement to use material that, while legal, could reasonably be considered by others, to be offensive, discriminatory, obscene, indecent or similar. Under these circumstances you should be mindful of other policies in this area e.g. Code of Practice on Research Ethics; and in the event that you require guidance, consider consulting your Dean or Course Leader to avoid possible issues later on.

The University reserves the right to monitor and block access to content considered illegal or that poses a security risk to the University IT systems.

# MONITORING

Equipment used on the UAL network will be monitored for adherence to regulations, operational efficiency, performance, and protection from malicious and illegal activities. Monitoring will be in line with the Regulation of Investigatory Powers Act 2000 and adhere to the Data Protection and the Human Rights Acts.

# LOSS, THEFT OR DAMAGE TO UNIVERSITY IT EQUIPMENT

You must report any loss, theft or damage of University owned IT equipment to your Course Leader or loan store immediately. This will enable access to the device to be revoked and/or the activation of any remote locate and wipe facility. In the event of theft you should obtain a Crime Reference Number by reporting the theft to the police.

# YOUR EMAIL OBLIGATIONS

The use of email carries similar obligations to any other kind of publication or commentary and should follow the same standards of professional practice and conduct associated with everything else we do. Common sense and sound judgment will help to avoid the most difficult problems. You should always assume that email messages may be read by others and you should not include anything that would offend or embarrass any reader, or you, if it found its way into the public domain.

Users of the University's systems must not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a student or member of staff via email, should inform their Course Leader.

The University reserves the right to suspend a user's email account as a result of any suspected misuse or breach of this policy.

# DISCLOSURE OF IT SECURITY

Students must not in any way publicly disclose any information about the security measures used to protect the University's information and IT networks that could be used by unauthorised persons to access the University's systems; or otherwise infiltrate, damage or compromise them. More specifically, this relates to disclosing technical information about how IT security is configured and implemented at a practical

level, or any known weaknesses which could be exploited by a third party regardless of whether the University is already aware of them.

## PERSONAL USE OF UNIVERSITY IT SERVICES

IT services such as email and internet access will be provided to students solely for the purpose of supporting University business and learning. You may make reasonable personal use of computing facilities provided by the University, as long as it does not interfere with the performance of your duties, does not damage or interfere with the smooth running of University IT services, or commit the University to additional costs arising from your personal use.

## COPYRIGHT INFRINGEMENT

When using externally sourced content such as images, text, music and software, you should consider any copyright or intellectual property right implications before using the content in your own work. The onus is on you to ensure that you use content within copyright law.

# RESPONSIBILITY

It is the responsibility of individuals to ensure that they comply with this policy. The rules and guidelines set out in the policy will be incorporated into the registration phase of all new students.

# BREACH OF POLICY

Security and information breaches arising from your failure to follow the guidance and terms of this policy will be considered a policy breach. Breaches will be logged and investigated in accordance with the University's Disciplinary Code for Students. In some cases this could lead to disciplinary action which, in cases of gross misconduct, could include immediate suspension pending a disciplinary hearing and possible expulsion in the case of students.

# Appendix A:

## DOMESTIC LAW RELEVANT TO THE USE OF IT SERVICES

When using UAL IT services you remain subject to the laws of the land, even those that are not apparently related to IT such as the laws on fraud, theft and harassment. There are many items of legislation that are particularly relevant to the use of IT, including:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and 2013
- Terms for the provision of JANET network services (including Eduroam and JISC Collections)
- Counter Terrorism and Security Act 2015

JISC provide an excellent set of overviews of law relating to IT use which is available at www.jisclegal.ac.uk/LegalAreas