UNIVERSITY OF
FORWARD
THINKING
WESTMINSTER

# IT Security & Use Policy

## 1. Introduction and Scope

This Information Technology (IT) Security & Use Policy forms a key part of the University's overall Information Security Policy. It governs how an authorised user can make use of, or access, the University's information systems and services.

**All users must accept this policy to make use of, or access to, the University's information systems and services.**

1.1 This policy applies to users of all University IT facilities:
- Any member of the University's staff, including Visiting Lecturers
- Any enrolled student of the University
- Members of partner institutions (e.g. WIUT)
- Any other party (including UWSU and Alumni) properly authorised to access the facilities.

1.2 This policy applies to use of all University IT facilities, including hardware, software, networks, information and service, whether
- Provided and managed by Information Services
- Provided and managed at a faculty or other local level
- Provided using the University's own resources, or by a contracted service partner.

1.3 This policy applies to access to all University IT facilities, including hardware, software, networks, information and services, including by equipment provided by the University, by the user him/herself or by any other party, in any location.

1.4 Users of IT systems and services at the University of Westminster have the ability to create, store and access a wide range of electronic information. The aim of this policy is to ensure that IT is used appropriately so that:
- Appropriate confidentiality is safeguarded.
- Access to systems and information is correctly authorised.
- The integrity of information is maintained. Information is accurate, up to date and not deliberately or inadvertently damaged. Appropriate controls are in place to protect information from internal and external threats.

- Information is managed as a valued asset and is available to support the users in their role within the University.
- The reputation and brand of the University is protected.
- Individual user's rights are respected.
- Data access and use conforms to relevant legislation and regulations, including the Data Protection Act 1998.

1.5 The University reserves the right to investigate any activity that is, or appears to be, in breach of this policy. Breaches of this policy will result in action under the University's Academic Regulations and Disciplinary policies and procedures, including:

- Academic Misconduct – Undergraduate and Postgraduate Taught Courses
- Academic Misconduct – Research (Staff)
- Student Disciplinary Procedure
- Staff Disciplinary Procedure

1.6 The University reserves the right to refer breaches of the law to the Police.

1.7 Any member of the University who is unsure what the policy means for them should seek advice from their Faculty Registry Office or Tutor (students) or from their line manager or the Information Security and Compliance Team (staff)

## 2 Authorisation and Registration

With the exception of information published on the University's public Web Site, access to the facilities is provided via a system of authorisation and registration, leading to the provision of an individual UserID and Password.

2.1 Students are allocated a UserID and initial password automatically as part of the University's enrolment process.

2.2 Staff (paid through payroll) are automatically issued with a UserID and initial password as part of the University's induction process.

2.3 Other authorised persons including partners, consultants, external examiners and contractor staff are issued with a UserID and initial password after completion of a non-staff access request form and its approval by a Head of Unit or Department.

2.4 Visitors to the University may be allocated a UserID and password for the duration of their visit. After this period the User ID account will be deleted.

## 3. UserIDs and Passwords

3.1 Initial passwords are valid for not more than 6 sessions, and must be changed on first access to the account.

3.2 All other passwords expire as follows:

- After 365 days (students)
- After 90 days (staff)
- At the end of the agreed period of access (visitors, temporary and contract staff)

3.3 If the user believes or suspects that his/her University account has been compromised or the password become known to any other individual (s)he must inform the FIXIT Service Desk immediately, and the password must be changed.

3.4 Personal Credentials: UserIDs and passwords are for the exclusive use of the account holder, and must never be shared.

3.5 It is a breach of this policy to:

- Share your allocated credentials with another user or users
- Use the credentials issued to another user

3.6 Users should never be asked to divulge a password, even for diagnostic or other technical purposes, by the first line support team (FixIT), other members of Information Services, or by line management. The user will be held responsible for any unlawful action or other breach of this policy carried out using his/her credentials.

## 4. Closure of Accounts

4.1 Student files and access are normally removed when the student‘s enrolment ceases. The University will not be responsible for the retention of data beyond this time.

4.2 Staff access will be disabled when the contract of employment is terminated at the end of the notice period. The University will not be responsible for the retention of data beyond this time. Line managers are responsible for ensuring the HR Leavers Checklist is followed to ensure business critical data and information is retained.

## 5. Access to Facilities

5.1 On-site IT facilities will be accessible during published opening hours, or in certain circumstances by special arrangements.

5.2 Many facilities can be accessed remotely, and may be available at any time. Information Services reserves the right to interrupt or withdraw services for planned or emergency maintenance. Details of planned maintenance are published in the University calendar.

## 6. Acceptable Use

6.1 Users must:

- Comply with the terms and conditions of all license agreements. Specifically, commercial use of University hardware and software is forbidden without prior authorisation from Information Services.
- Comply with any instructions or regulations displayed in and around computing facilities.
- Comply with the JANET Acceptable Use Policy (see http://www.ja.net/documents/publications/policy/aup.pdf)
- Understand that the University reserves the right to check for insecure and vulnerable devices connecting to its wireless or wired network infrastructure and to block access from such devices.
- Use University provided services for official business, such as email and provided storage areas.

6.2 Users must not:

- Cause any damage to the facilities. These include hardware and software, IT Laboratories and Open Access computing suites, the network wiring infrastructure and communications equipment. The term "damage" includes any unauthorised modifications to hardware, software or infrastructure. All costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements will be charged to the person or persons causing the damage. The University will determine the costs.

- Introduce any virus, worm, malware, trojan horse or any other "nuisance" program such as file sharing or peer-to-peer software to any University system or take any action to circumvent or modify any precautions taken by the University to prevent "infection" of its machines
- Use the IT facilities for creating, sharing, sending or storing any textual or graphic or voice or video content that is offensive, abusive, obscene, defamatory, racist or unlawful
- Access, or attempt to access, any facilities without authorisation
- Connect any equipment to the University wired network that is not managed by information services without prior approval
- Move any fixed equipment from its designated place.

6.3 The University may at any time permit the inspection, monitoring, or disclosure of Information held in IT Facilities:

- When required by and consistent with the law. The University evaluates any request for such action against the precise provisions of the Freedom of Information Act 2000, Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, or other applicable law.
- At the written request of the University Registrar and Secretary, the Deputy Vice Chancellor or a Dean of Faculty if there are reasonable grounds to believe this policy has been violated.
- At the written request of the University Registrar and Secretary, the Deputy Vice Chancellor or a Dean of Faculty in support of a bone-fide internal investigation instigated under another of the University's Policies.

6.4 Any such monitoring, access or investigation will be carried out by an appropriate and competent member of Information Services staff under the guidance of the Head of Information Security and Compliance.

6.5 The University also reserves the right to carry out system management, problem resolution, maintenance and capacity planning to ensure the performance and availability of its systems.

## 7 Policy Approval

7.1 Authorised by: University Information Governance Group
Date: 21st May 2014

UNIVERSITY OF
FORWARD
THINKING
WESTMINSTER

7.2 Authorised by: University Information Management Group
Date: 26th June 2014

7.3 Authorised by: University Executive Board
Date: 1st October 2014

| Version | Author | Publication Date | Description |
|---|---|---|---|
| V3 | Information Security & Compliance, as amended by Information Management Group | 1st May 2015 | The IT Security & Use Policy |

.

**REVIEW DATE:** 1ST OCTOBER 2015

UNIVERSITY OF
FORWARD
THINKING
WESTMINSTER

**Appendix A - Relevant Statutes and other Regulations**

It is the policy of the University that all of its activities are conducted in accordance with current legislation; a list of relevant statutes and other regulatory requirements is provided here.

This policy is informed by recommendations from JISC and UKERNA and by the UCISA Information Security Toolkit. It is in line with ISO27001 best practice for Information Security.

Users of the University's information systems should be aware that the Data Protection Act (1998) covers their personal actions when processing personal data (information relating to a living person). Further information and guidance may be obtained from the University's Data Protection Officer: DPA@westminster.ac.uk or from the website of the Information Commissioner's Office: https://ico.org.uk

The Copyright, Designs and Patents Act 1988
The Data Protection Act 1998
The Human Rights Act 1998
The Computer Misuse Act 1990
The Regulation of Investigatory Powers Act 2000
The Freedom of Information Act 2000
The Electronic Communications Act 2000
The Digital Economy Act 2010
The Obscene Publications Act 1959
The Sex Discrimination Act 1975
The Race Relations Act 1976
Disability Discrimination Act 1995
Part-Time Workers (Prevention of Less Favourable Treatment) Regulations 2000
Fixed-Term Employees (Prevention of Less Favourable Treatment) Regulations 2002
Employment Equality (Sexual Orientation) Regulations 2003
Employment Equality (Religion or Belief) Regulations 2003
Harassment Act 1997
Employment Equality (Age) Regulations 2006
The Protection of Children Act 1978
The Public Order Act 1986
The Criminal Justice and Public Order Act 1994
The Terrorism Act 2006
Counter-Terrorism and Security Act 2015

Together with various Statutory Instruments and other pieces of legislation