UNIVERSITY OF
WEST LONDON

# Information Security Policy

| | |
|---|---|
| **Responsibility of**: | IT Services |
| **Approval Date**: | 10 November 2020 |
| **Review Date**: | November 2021 |
| **Approved By**: | IT Steering Group (ISG) |

# Foreword

The University of West London (UWL) has an ethical, legal and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity and availability. In other words, the information UWL is responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it. This information security policy sets out its approach to information security management.

In today's highly connected, highly electronic world, information is generated and used everywhere from the point at which a prospective student first makes contact with UWL and then right the way through the student journey to alumni. Data can underpin research and intellectual property. It also supports the management of the institution. Sharing data is easier than it ever has been and more and more people chose to access systems (and therefore data) through personal devices.

UWL considers information to be a strategic asset that is essential to its core mission and objectives. It has a responsibility to manage effectively the risks around protecting the confidentiality, integrity and availability of its data and in complying with all statutory, regulatory and legal requirements.

The Information Security Policy set out bellow is an important milestone in the journey towards effective and efficient information security management. It sets out the responsibilities we have as an institution, as managers and as individuals. It has, therefore, my full support and I expect all UWL staff, students and anyone else who has access to UWL information to read it and abide by it.

Professor Peter John
Vice Chancellor & Chief Executive

University of West London

# Introduction, Purpose, and Scope

## 1. Introduction

1.1. The University of West London (UWL) has an ethical, legal and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity and availability. In other words, the information UWL is responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it.

1.2. This information security policy outlines UWL's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the University's information systems.

1.3. Under that umbrella, supporting policies, procedures and guidelines provide further detail on how to implement those information security arrangements.

## 2. Purpose

2.1. The main purpose of this policy is to describe the minimum level of protection that UWL expects from all UWL's information systems to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

2.2. A secondary but very relevant purpose of this policy is to ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle, including making users aware of relevant legislation.

2.3. The directives set in this policy are defined in the context of the overarching objectives of information security at the university, which are:

- To support the Institutional business objectives in a flexible and effective way
- To maintain adequate regulatory compliance
- To protect UWL's information assets and protect information systems from unauthorised access, use, disclosure, destruction, modification, disruption or distribution.
- To maintain business continuity

2.4. The UWL Senior Management Group will ensure business, legal, regulatory requirements and contractual information security obligations are met.

2.5. The university's information security activities will be monitored regularly with regular reporting of the status and effectiveness at all levels.

2.6. This policy is the cornerstone of UWL's on-going commitment to establish and maintain our information security procedures.

## 3. Scope

3.1. This policy is applicable, and will be communicated to all staff, students, other members of UWL and third parties who interact with information held by the UWL and the information systems used to store and process it. This includes, but is not limited to, any systems or data attached to the UWL data or telephone networks, systems managed by UWL, mobile and personal devices used to connect to UWL networks or hold UWL data, data over which UWL holds the intellectual property rights, data over which UWL is the data owner or data custodian, and communications sent to or from UWL.

## Roles and Responsibilities

### 4. Responsibilities of every user of UWL resources, including third parties

4.1. Staff, Students and – in general – users of UWL IT resources are expected to meet the acceptable usage policies and related terms and conditions of the services provided by UWL and by any third party on our behalf (e.g. Janet acceptable use policy, Microsoft software licensing agreements).

4.2. The University will provide tools to create and store data, and to connect to the Internet and other networks. Users must apply these in a legal and appropriate manner, to protect the personal safety of themselves and their peers and to ask the University staff for advice or assistance in case of doubt or concerns. The IT Service Desk should be the first point of contact.

4.3. Users must manage passwords with care and in line with the Password Policy.

### 5. Responsibilities of staff members

5.1. All employees and third parties using UWL systems are accountable for understanding and following UWL's information security policies, as well as promoting safe practices within their teams and monitoring compliance.

5.2. All employees and third parties are responsible for asking for assistance when in doubt about how to proceed or interpret a policy and also to report any concern or suspect activity encountered. Depending on the nature of the concern, the first point of contact should be one of these: the line manager, IT Service Desk, the Information Security Manager or Human Resources.

### 6. Responsibilities of managers

6.1. UWL managers are expected to identify the data and systems under their remit and accept accountability for their protection. Individual "custodians" (also referred as "owners") of the data will be identified. They will be accountable for it and will make informed decisions on risks and appropriate levels of protection, on behalf of the University.

6.2. UWL managers should not exclusively rely on perimeter controls, but also implement (or fund) security on each individual system. In an open and dynamic organisation such as UWL, having a clear strategy of providing flexible and seamless mobile access, it is no longer effective to rely on broad "Internet vs internal" networks, on restricting physical access to the campus, or on attacker ignorance of our estate and IT tools to protect UWL from accidental or intentional misuse.

6.3. UWL managers that sponsor a system to process UWL data are accountable for commissioning one that meets the information security policy and the data protection policy, applying deliberate and verifiable risk management. Security measures need to be identified, designed, resourced and delivered from the start of any initiative alongside any other business functionality and maintained for the entire lifecycle of the process or IT system, up to the data and system disposal.

6.4. Professional service functions such as IT Services, Human Resources, Legal and Finance will support the delivery of security on an "internal service provider" model. These functions will have also the mandate to monitor compliance and where appropriate will have accountability for the custodianship/gatekeeping in maintaining the practices agreed/accepted by Vice-Chancellor's Executive.

6.5. UWL managers should ensure that the risks of concentrating functions on a single control ("single point of failure") - whether performed by individuals or systems- are well understood and actively managed. Managers need to choose and implement the combination of preventative and monitoring controls that best meet the business objectives.

6.6. UWL managers should ensure their teams have the necessary skills and should communicate their responsibilities regarding protecting systems and data.

6.7. UWL managers should actively, regularly and demonstrably verify what their reports are doing and how systems under his/her supervision are functioning (with the assistance of IT Services where appropriate).

6.8. UWL managers should ensure any subcontractor employed for a particular function will meet the requirements specified (on selection and on an ongoing basis) and accept responsibility for their actions.

## 7. Responsibilities of senior management

7.1. The Vice-Chancellor's Executive owns the overall risk management process, and the prioritisation and acceptance of risks. Risks are identified "bottom up" from each department and "top down" from the Vice-Chancellor's Executive in a two-way flow.

7.2. Heads of School, individually or via governing bodies, have the accountability for taking a stance on risks within their authority (or escalating if exceeds it) and ensuring the business operates in line with the Vice-Chancellor's Executive expectations.

7.3. Governance arrangements, such as the Audit & Risk committee of the Board of Governors, the Information Governance Group, and the Internal Audit programme, will help to identify risks to the University. The Vice Chancellor's Executive will take advice from these and other sources, including the University's own Risk Register. Ultimately the responsibility for risk lies with the Vice- Chancellor's Executive.

## 8. Responsibilities of the Information Security Manager

8.1. The Information Security Manager will identify threats to the University's information assets and advise the Audit & Risk Committee and the Information Governance Group on impact and recommended remediation. Scope includes risks related to information, data, technology & related regulatory requirements.

8.2. The Information Security Manager will communicate acceptable levels of risk and mitigation practices throughout the University via policy, standards and awareness programs. Central initiatives to communicate, facilitate/enable the adoption of secure practices.

8.3. The Information Security anager will validate compliance with information security requirements either directly on processes or by verifying management controls.

8.4. The Information Security Manager will develop central capabilities to effectively respond to significant information security related incidents.

8.5. There may be central services delivered by the Information Security Manager, for example on demand pen testing, or some diagnostics/checks.

### 9. Responsibilities of third-party providers

9.1. Third parties shall adhere to the information assets - acceptable usage policy as well as any other requirements specified in the service contract.

9.2. Third parties working for UWL are expected to participate in incident response tests or drills as any other member of staff, when using UWL resources and/or premises. Specific audit/reviews/checks might be undertaken on external service providers, due to the dynamic nature of such relationships.

## Policy

### 10. Organization of Information Security

10.1. The Vice-Chancellor's Executive has the ultimate accountability for implementing information security at UWL.

10.2. The IT Steering Group (ISG), with Vice-Chancellor's Executive representation, oversees the strategic development of IT Services and solutions at the university, including Information security.

10.3. The Information Governance Group (IGG), chaired by the University Secretary and Chief Compliance Officer, maintains an overview of information governance within the University and reports to VCE.

10.4. The Information Security Manager leads the information security function and has remit across the University. They will support departments to require evidence or perform direct validation of compliance against policy. Specific sign-off requirements by the Information Security Manager may be established in policies or operational procedures.

10.5. Appropriate contacts with industry groups or other specialist security forums and professional associations should be maintained. Leverage of UWL's own academic expertise should be sought, where appropriate.

10.6. Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

### 11. Policy Management, Education, and Awareness

11.1. Managing risks is an essential part of the business activity at all levels of the organisation. The information security policies are only the minimum expectation to address information security risks according to well established practice. Management should assess the business, legal, contractual and corporate social responsibility risks and requirements in each relevant jurisdiction to decide on the need for additional controls or exceptions and be able to justify and be accountable for these decisions. The risks management process will follow the UWL risk management policy and be reviewed formally at least annually.

11.2. A set of policies and procedures for information security will be maintained, approved by management, published, and communicated to employees and relevant external parties. These policies should follow the overarching framework for policy approval and review defined at UWL level. In particular, policies should be reviewed and updated at least annually.

11.3. The policy statements are necessary but not sufficient on its own. There needs to be controls in place to provide comfort that policies are being followed. Furthermore, those controls should not be transactional or preventative only; managers should perform demonstrable “controls over the controls” at an appropriate level of detail to reasonably conclude they are effective.

11.4. Managers should ensure staff and external parties working with UWL systems and data are formally aware of and educated on the policies and procedures they must be compliant with. This is a fundamental step to establishing any individual’s accountability.

## 12. Human Resource Security

12.1. Every employee and third party granted access to UWL systems and/or data has a responsibility to use the systems and data in a secure manner, for UWL business purposes, following UWL policies and applying good judgment. Only approved hardware, software and data should be used to perform UWL business. The extent and exceptions to this policy, including personal use of UWL resources is defined in the UWL information assets - acceptable usage policy.

12.2. Users are responsible for reporting any concern on how the security processes are performing, any suspected or confirmed incident regarding unauthorized or incorrect use to their manager, the IT Service Desk, the Information Security Manager, or Human Resources.

12.3. Management is responsible for requiring their teams of employees and contractors to apply information security according to established policies and procedures, and to monitor use within his/her teams, leading by example and ensuring their direct reports have been educated on policies and security practices.

12.4. Background verification checks on candidates for employment, employees or contractors, as established by Human Resources, shall consider explicitly the sensitivity of the information to be accessed and the perceived risks when defining the nature and timing of those checks.

12.5. The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security including those that remain after termination or change of functions. Detail procedures should be documented and communicated to the employee or contractor and enforced.

12.6. The HR department is responsible for defining and communicating the disciplinary process applicable to employees who have committed an information security breach.

## 13. Data/Assets Management

13.1. Each department manager must identify the data being used for fulfilling their duties and adopt controls to protect the information according to its risk. Assigning ownership and a sensitivity classification is a highly recommended method of protecting assets efficiently. If no formal classification is used, the department should work on the assumption that all information is as critical as the most critical information they possess.

13.2. UWL will have processes in place to safely dispose of information as required by law or, within legal compliance, when is no longer cost effective to retain. Based on their remit, Managers, assisted by legal counsel, is responsible for defining the acceptable retention period for the various kinds of data they hold. Managers are also responsible for establishing the controls to ensure these criteria are followed.

13.3. IT services will define and put in place formal procedures for the safe acceptance, storage and disposal of surplus technology hardware (including electronic storage media). UWL only accepts new, vendor guaranteed equipment and destroys surplus/failed equipment/media/paper securely, compliant with the law, and (then) in an environmentally friendly way. Other arrangements need to be dealt on a case by case with business and technical signoff.

13.4. Property Services will define formal procedures for the safe storage, retrieval and disposal of paper files.

13.5. As a general rule, any logging activity should be kept for at least one year, of which three (3) months should be online immediately accessible upon request from a governing body or external inspection. Management needs to familiarise with local contractual/legal requirements applicable to each business to determine if additional requirements apply, or a shorter retention is acceptable.

13.6. UWL assets, including systems and media need to be protected against intentional or accidental physical damage. For that, they will be located in an area with restricted access and protected against environmental hazards, under full control of UWL.

## 14. Security by Design, Secure Architecture, Acquisition and Development

14.1. IT Services will establish the approved technologies and design principles that can/should be deployed in UWL or vet specific solutions during the project, following and IT architecture methodology. Approval by IT Services or ultimately the Vice-Chancellor’s Executive must be obtained for exceptions.

14.2. Information security and data protection shall be addressed in project management explicitly as a requirement, regardless of the type of the project, and will be incorporated into the methodology.

14.3. The default and vendor recommended configuration of any acquired system should not be trusted but subject to review and security lock down by an employee or independent reviewer with sufficient expertise. The reviewer will be responsible and accountable for commissioning a system sufficiently secure for its purpose.

14.4. There must be separate development, test, and production environments for all business-critical applications, with appropriate segregation of duties. These environments must be kept separate by system-enforced security measures appropriate to protect the sensitivity of the software. In addition to protecting live data, attention should be given to protecting test data, migration data and approved source/object code.

14.5. The default approach is that all UWL systems should have detection, prevention and recovery controls to protect against malware combined with appropriate user awareness. Exceptions need to be formally approved on a case by case basis by senior management from IT and the business affected

14.6. Systems should be developed/acquired and configured with the security features necessary to enable enforcement of the following:
a) Users can only access data and functionality for which they are authorised (“least

privileges" approach)
b) Accountability for usage is maintained via appropriate audit trails.
c) Availability and integrity of the systems, including disaster recovery (DR) arrangements are addressed.

14.7. These security requirements need to be made explicit, should follow UWL project management and architecture methodology and should be included in services agreements, whether these services are provided in-house or outsourced.

14.8. All systems must be developed/configured following practices that specifically identify and minimise vulnerabilities, and subsequently, processes will be in place to promptly address newly discovered vulnerabilities according to their criticality.

14.9. Software installation should be restricted to users approved by IT Services. Only licensed and supported software approved by IT Services is allowed to be installed on systems in line with the UWL patch management policy. Installation of software updates should be managed by IT Services and follow the standard (or emergency) change management process and the UWL patch management policy.

14.10. The IT security of IT systems should be tested as part of the regular business as usual. Systems should be probed for vulnerabilities before the go-live or significant change, and at least annually afterwards (special regulatory requirements may apply).

14.11. Every asset in the network should be configured securely individually as well as protected by a network architecture that secures the perimeter and incorporates segregation of environments. The design should aim at minimising weak links or "single points of failure" by establishing resilient, redundant, complementary controls, separation of duties, etc. Specific measures need to consider the risks and criticality/value of the asset protected, balancing usability and regulatory requirements.

## 15. Technical and Operational Security

15.1. Additional security measures should be put in place to grant, revoke/restrict, authenticate and monitor usage of remote, mobile access and "bring your own device", compared with on-site "wired" access from a fully owned UWL device. At a minimum, the technology used to access UWL systems need to be approved by IT and the line manager of the user, prior to using/granting such access. Management approval must be documented and explicit (i.e. not available by default).

15.2. Only IT Services approved tools and methods will be used to encrypt data UWL have ownership or custodianship of. Data owners are responsible for selecting an approved encryption method and ensuring the recoverability of the data and safeguarding of the encryption keys, in consultation with IT. Minimum requirements for encryption are defined in a separate technical policy, in alignment to the UWL data classification model.

15.3. IT Services and the business management that owns the system have a joint responsibility for defining operational procedures and training users to ensure the secure operations of the processing facilities.

15.4. Changes and tests on live (i.e. production) systems including servers and end-user devices should be conducted in a controlled manner. Direct changes in production, un-announced tests/hacking, or intentionally creating a failure are not authorised by default.

15.5. IT Services has a mandate to monitor the performance, integrity and overall confidentiality of the systems and have the technical knowledge and authority to apply measures to protect the overall infrastructure against threats, following normal or emergency procedures.

15.6. UWL reserves the right to monitor individual’s usage, to the extent granted by the law, in order to protect its legitimate business interests. Monitoring may include accessing stored or transmitted data as well as observation of user activity.

15.7. UWL has also a "duty of care" obligation to reasonably monitor usage of company resources to detect abuse in breach of the law, and to report to the appropriate authorities.

15.8. By default, system logs should be enabled to capture user logon, exceptions, faults and information security events/alerts. Regulatory and audit/compliance requirements involving logging, audit trails, reporting and any other functionality/processes to enable verification of operational systems are a mandatory requirement to be assessed explicitly in any systems project.

15.9. All changes to production data and programs must be done following a documented change management process, and security should be in place to enforce that process via automated controls where possible.

15.10. Equipment shall be installed with appropriate protection from environmental factors and unauthorised access, in line with the sensitivity of the data and business process it supports. All equipment by default should be provisioned, installed and managed by IT Services, with vendor warranty and maintenance in place. Exceptions, including vendor managed installation and pre-approved decentralised purchases, need to be reviewed by IT Services and approved on a case-by-case basis.

15.11. Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup plan approved by the data/system owner. As a default/minimum criterion, backups plans should allow restore at any point of the past 30 days, plus last 12 months of monthly snapshots and 7 years of annual copies, stored in a different location than the system being backed up. Backups should be stored encrypted, under physical security and inventory control. Restore tests of the media/files should be done at least once a year.

## 16. Access Management

16.1. Access to UWL systems and data should be granted on a "need to know basis", that is, the minimum access needed to perform a duty. This is to protect the systems and data in them from accidental or intentional loss.

16.2. Access to systems and information, including setting up permanent network connectivity solutions, will be granted to employees and third parties/service providers only after a due diligence risk assessment has been performed and after the employment or service contracts, including confidentiality and accountability clauses has been agreed in writing. Processes should be in place to ensure ongoing monitoring of compliance.

16.3. Each Business Unit must have a consistent process to approve modify and remove, as well as regularly review the access granted to users on systems and information he/she is accountable for, and monitor the usage of the system, with assistance and tools provided by IT.

16.4. All enabled accounts in computer systems must have passwords or a comparable authentication method to establish user accountability. If using passwords, these need to have system enforced complexity, expiration, reuse and lockout controls in line with the UWL password policy. System enforced session timeout is required. Passwords and other secret information needed for authentication should not be transmitted over the networks or stored in the clear (i.e. needs to be securely hashed or encrypted).

16.5. Systems and procedures should ensure activity in the systems or with IT assets can be linked to an individual. When the individual is not an employee, the manager accountable for allowing and monitoring such access should be clearly identified. If the account is used by another system, there still need to be an appointed individual responsible for the setup and system credentials and generally the safeguarding of that account.

16.6. All employees and third parties using UWL's systems are accountable for understanding and following UWL's security policies, in particular on how to protect their accounts and passwords from misuse. All employees are expected to report any concern or potential suspect activity they may encounter. Employees should contact their line manager, IT or Human Resources for clarification or assistance.

16.7. All privileged/administrator activity (e.g., ID and password creation, direct access to data, maintenance, and support) must be traceable to the individuals whether directly accountable for these activities, or indirectly accountable, in the case of automated processes. Management of such accounts must be caried out in line with the UWL privileged account policy.

## 17. Incident Management

17.1. UWL will maintain an information security incident response plan that will rely on ongoing operational monitoring and incident response procedures, including escalation procedures to senior management and integration with the UWL institutional continuity management plan.

17.2. Appropriate contacts with relevant authorities and external entities (e.g. the Press) shall be maintained. In case of an incident, only nominated contacts are authorised to liaise with authorities and external entities, following the protocols defined in the UWL incident response plan and/or instructed by the Vice-Chancellor's Executive.

17.3. If a member of the University (staff or student) is aware of an information security incident or near miss, then they must report it to the IT Service Desk. If necessary, members of the University can also use the institutional whistle blowing process (see Public Interest Disclosure policy).

## 18. Continuity Management

18.1. People, assets, and information services need to be protected in a disaster situation; to save lives and to ensure the continuity of the going concern. For that UWL establishes and maintain a business continuity plan.

18.2. Information Security shall be embedded in the continuity plan to ensure operations, even during an adverse situation, maintain acceptable levels of security and meet regulatory requirements.

18.3. Managers are responsible for specifying the requirements for protecting the availability of systems/data and ensuring the necessary funding to implement these is in place, and are ultimately accountable for its implementation. It should be based on the analysis of risks, criticality of assets and consider regulatory requirements. IT Services responsibility is to deliver and maintain the contingency arrangements as agreed.

18.4. Resilience and disaster recovery capabilities are an integral part of all IT services and need to be defined in the design phase of any project.

18.5. Disaster recovery capabilities are especially vulnerable to failure and will not be deemed acceptable unless they pass regular documented tests.

## 19. Compliance, Validation and Certification Initiatives

19.1. UWL and each employee is accountable for operating within the law, and it is their responsibility to be aware of legal and contractual requirements and implement the controls within their remits to comply.

19.2. Service Providers with access to UWL systems and data must contractually commit to implement security measures to meet the business objectives (e.g. protecting intellectual property, availability) as well as regulatory or contractual obligations for which UWL has ultimate accountability.

19.3. The manager that owns the service is responsible for regularly monitoring, review and audit supplier service delivery. Information Security considerations, including protecting UWL intellectual property and maintenance of regulatory compliance requirements should be explicit in this review.

19.4. Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Evidence of the performance of such controls should also be kept.

19.5. The information security control framework shall be reviewed independently at planned intervals or when significant changes occur. It is expected that evidence of the controls performed by employees/systems as well as any controls management performs over them (also called “second tier” or “control over the control”) are kept. Management should be prepared for -and fully cooperate during- internal reviews performed by Internal/External Audit and the Information Security Manager.

19.6. UWL specifically acknowledges the contractual requirement to handle payment card details of UWL customers securely and with care and meet the appropriate data security standards maintained by the PCI Council.

## 20. Guidance On Legal, Regulatory and Contractual Obligations

20.1. Relevant legislation to consider (please note this is not a complete list and laws are constantly enhanced with modifications or underlying administrative procedures):

- Agreement on Trade-related Aspects of Intellectual Property 1994

- Broadcasting Act 1990
- Computer Misuse Act 1990
- Communications Act 2003
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Software) Amendment Act 1985
- Copyright Directive 2001/29/EC
- CE Convention on Cybercrime 2001
- Criminal Justice Act 1988
- Criminal Justice and Immigration Act 2008
- Counter-Terrorism and Security Act 2015
- Data Protection Act 2018
- Defamation Act 1996
- Digital Economy Act 2017
- Directive on Copyright in the Digital Single Market
- Electronic Commerce (EC Directive) Regulations 2002 (2000/31/EC)
- Electronic Communications Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1964
- Police and Criminal Evidence Act (PACE)
- Prevention of Terrorism Act 2005
- Protection of Children Act 1978
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 and 2004 Amendment
- Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Freedom of Information Act 2000
- The Telecommunications (Data Protection and Privacy) Regulations 1999
- Terrorism Act 2000
- Terrorism Act 2006

- The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

## 21. Administration, Maintenance, Communications

21.1. As defined in the policy, this set of documents is maintained by the Information Security Manager and is to be reviewed annually. The Information Security Manager, in coordination with Human Resources and Legal counsel will announce the exercise, which will involve representation of Academic, Non-Academic and Student bodies.

21.2. The review and update will be approved by the ISG group.

21.3. Every new employee will have this policy included in the induction pack. After each review, the news of the policy update will be communicated to all employees

21.4. The current approved version of this policy will be published in the UWL Internet site. Previous versions will be kept by the Information Security Manager.

## 22. Enforcement

22.1. This Policy forms part of the UWL set of policies every employee needs to understand and follow as indicated in the standard employment contract.

22.2. Failure to follow the policy may lead to disciplinary action, led by Human Resources.

## 23. Supporting Policies, Procedures and Guidelines

23.1. Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated procedures and guidelines are published together and are available for viewing on the UWL's website in the Policies section.

23.2. All staff, students and any third parties authorised to access UWL's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

23.3. The relevant supporting policies and standards are:

- Access to User Data Policy (pdf, 54kb)
- Bulk email policy (pdf, 28kb)
- CCTV Policy (pdf, 396kb)
- Data Protection Policy (pdf, 354 kb)
- Data Retention Policy (pdf, 203 kb)
- Information assets - acceptable use policy (pdf, 83 kb)
- Password Policy (pdf, 134 kb)
- Patch Management policy (attached as addendum)
- Prevent duty page
- Privileged Account Policy (pdf, 94kb)
- Public Interest Disclosure Policy (Whitstleblowing) (pdf, 213 kb)
- Records Management Policy (pdf, 200 kb)
- Risk Appetite Statement (pdf, 312 kb)
- Risk Management Policy (pdf, 265 kb)
- Safeguarding Children Policy (pdf, 529 kb)
- Social Media Policy for Staff (pdf, 81kb)

- Supply of IT equipment policy (pdf, 130 kb)
- Student Handbook
- Student Code of Conduct (pdf, 112.32 kb)
- Staff Disciplinary Policy and Procedure (pdf, 376 kb)
- User Account Lifecycle Policy (pdf, 66 kb)
- Web Filtering Policy (attached as addendum)

UNIVERSITY OF
WEST LONDON

# Web Filtering Policy

| | |
|---|---|
| **Responsibility of**: | IT Services |
| **Approval Date**: | August 2020 |
| **Review Date**: | August 2021 |
| **Approved By**: | IT Steering Group |

# 1 Introduction

1.1 The University strongly support the principles of Academic Freedom and wants staff and students to be able to use the web freely as part of their studies.

1.2 But the University also has responsibilities under the PREVENT duty, for child safeguarding, and to protect University systems and data from harm and cyber-attack.

1.3 UWL has the technical capability to apply filters to web browsing at both the campus network and endpoint level. Filters can be configured to block individual web sites, or to block based on vendor-supplied and updated lists of web sites falling into pre-defined categories such as Drugs, Gambling, Violence, and Pornography.

1.4 Our use of Web filtering technology must balance these considerations.

# 2 Policy

2.1 UWL will not generally filter access to the web for staff and students, with two important exceptions.

2.2 We will block access to known malicious web sites in order to protect UWL from malware, phishing, crypto-jacking, and other forms of cyber-attack.

2.3 We will enable category-based filtering for FE students, since they may be under 18. See Appendix for a list of the categories blocked.

2.4 Younger students, such as those attending Junior College, are not issued UWL network accounts and so cannot access the web using UWL facilities.

2.5 Note that under-18s may be able to access the web on campus using personal devices with mobile data capability, and that this is beyond IT Services' control.

2.6 Should a member of staff require access to a blocked site for themselves or their students, they should contact the Information Security Manager to discuss their requirements.

2.7 While we do not generally filter access to the web, staff and students should be aware of and keep in mind their responsibilities under UWL policies, including the acceptable use policy, information security policy, data protection policy, safeguarding policy, and social media policy.

2.8 This policy will be reviewed at least annually.

## Appendix: Filtering categories for FE students

UWL uses the Paolo Alto PAN-DB URL filtering system.

This system allows us to identify categories of URLs which will be blocked for FE students. The lists of blocked URLs in each category are maintained and updated by Palo Alto.

We currently block the following categories:

| | |
|---|---|
| Abused Drugs | Sites that promote the abuse of both legal and illegal drugs, use and sale of drug related paraphernalia, manufacturing and/or selling of drugs. |
| Adult | Sexually explicit material, media (including language), art, and/or products, online groups or forums that are sexually explicit in nature. Sites that promote adult services such as video/telephone conferencing, escort services, strip clubs, etc. Anything containing adult content (even if it's games or comics) will be categorized as adult. |
| Alcohol and Tobacco | Sites that pertain to the sale, manufacturing, or use of alcohol and/or tobacco products and related paraphernalia. Includes sites related to electronic cigarettes. |
| Command and Control | URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker’s remote server to receive malicious commands or exfiltrate data. |
| Dating | Websites offering online dating services, advice, and other personal ads |
| Extremism | Websites promoting terrorism, racism, fascism or other extremist views discriminating people or groups of different ethnic backgrounds, religions or other beliefs.<br>Should not include websites discussing controversial political or religious views. |
| Gambling | Lottery or gambling websites that facilitate the exchange of real and/or virtual money. Related websites that provide information, tutorials or advice regarding gambling, including betting odds and pools.<br>Corporate websites for hotels and casinos that do not enable gambling are categorized under Travel. |
| Malware | Sites containing malicious content, executables, scripts, viruses, trojans, and code. |
| Nudity | Sites that contain nude or seminude depictions of the human body, regardless of context or intent, such as artwork. Includes nudist or naturist sites containing images of participants. |
| Phishing | Seemingly reputable sites that harvest personal information from its users via phishing or pharming. |
| Proxy Avoidance and Anonymizers | Proxy servers and other methods that bypass URL filtering or monitoring. |
| Weapons | Sales, reviews, descriptions of or instructions regarding weapons and their use. |

UNIVERSITY OF
WEST LONDON

# Patch Management Policy

|  |  |
|---|---|
| **Responsibility of**: | IT Services |
| **Approval Date**: | August 2020 |
| **Review Date**: | August 2022 |
| **Approved By**: | IT Steering Group |

## 3 Introduction

3.1 UWL has a sizeable IT estate and processes a great deal of information, including much that is sensitive or confidential. The devices and software making up this estate may have technical vulnerabilities that a cyber-criminal can exploit.

3.2 It is essential then that these devices and software:

- Are licensed and supported, so that the vendor produces security patches when they discover vulnerabilities
- Have those security patches applied in an appropriate timescale, determined by the severity of the vulnerability they fix, by whether the vulnerability can be exploited in the UWL environment, and by the required time for testing.

## 4 Policy

4.1 UWL will deploy all security patches marked as CRITICAL or HIGH severity by the vendor within 14 days of release. Where the vendor uses different terms to indicate severity, reference will be made to the definitions in the Common Vulnerability Scoring System (CVSS) to determine which patches are considered CRITICAL or HIGH.

4.2 Deployment of security patches marked as MEDIUM or LOW, and of non-security patches such as feature improvements or bug fixes, need not be done within 14 days but should be carried out regularly.

4.3 Where a vendor has marked a patch as CRITICAL or HIGH but other security controls are in place which mean that an attacker would be unable to exploit the vulnerability, they should normally still be deployed within 14 days but can, with approval of the CIO or ISM, be treated as MEDIUM severity.

4.4 All software in general use in the University should be licensed and actively supported by either the vendor or developer, or by a support contract with a third party. This applies to Free or Open Source (FOSS) software as well as to commercial software.

4.5 If it is necessary for the University to use software that is no longer actively supported then compensating security controls, such as network isolation, must be put in place and documented, in order to mitigate the risk.

4.6 Owners of systems that are not maintained by IT are responsible for ensuring their systems are patched according to this policy.

4.7 At regular intervals, and at least quarterly, internal vulnerability scans will be carried out by IT Services in order to identify any missing patches and unsupported software.

4.8 UWL may require that non-UWL devices be at a suitable patch level before connection to the campus network.