UNIVERSITY OF WESTMINSTER

Information Security Policy

1. Purpose

1.1 The Information Security Policy (the ‘Policy’) sets out the University of Westminster’s (the ‘University’) approach to information security management.

1.2 The Policy, and the supporting Information Security Framework set out in section 5 of this Policy (the ‘Framework’), support the strategic vision of the University and facilitate the protection of the University’s information and technology services against compromise of its confidentiality, integrity and availability.

1.3 Confidentiality: a component of privacy that protects our data from unauthorised access or disclosure.

1.4 Integrity: maintaining and assuring the accuracy and completeness of data over its entire lifecycle.

1.5 Availability: guaranteeing reliable access to information by authorised personnel when it is needed.

1.6 This Policy and the Framework advocate a holistic approach to information security and risk. This is achieved by identifying and assessing information security threats and developing and implementing a combination of people, process, and technology controls to mitigate information security risks according to the University’s agreed risk appetite.

1.7 The purpose of this Policy and the Framework is to form an effective Information Security Management System (ISMS) based on the International Standard ISO 27001:2013. This advocates a risk-based approach towards the implementation of appropriate levels of security controls in the University’s business functions and processes.

1.8 This Policy provides a structured approach to protect sensitive data, maintain regulatory compliance, and defend against cyber threats. It establishes clear guidelines and responsibilities, fosters security awareness, and helps safeguard the University's reputation and operations, ensuring academic and institutional integrity.

1.9 The ISMS allows us to:-

- Protect the interests and privacy of all our stakeholders.
- Contribute to our resilience and recovery capability.
- Secure our intellectual property and financial interests.
- Comply with relevant legislation.
- Uphold and maintain our reputation.
- Respond to inquiries and complaints about non-compliance of security requirements and data protection.

1.10 This Policy sets out the senior management commitment to information security and designates the appropriate roles and responsibilities across the organisation to protect information and information systems.

2. Scope

2.1 This Policy and the Framework apply to all information created, stored, processed, transmitted and disposed of in the course of University business in all formats, whether held or transmitted in paper, electronic formats or communicated verbally.

2.2 Information assets include, but are not limited to: databases, data files, documents, contracts and agreements, teaching materials, academic papers, research data, intellectual property, financial information, dissertations, system documentation, user manuals, training materials, operational/support procedures, risk registers, business continuity plans, backup plans, audit trails, emails, online chat records, video and audio records, archived information and IT systems.

2.3 This Policy and the Framework apply to all users of University information.

2.3.1 Users includes colleagues, students, alumni, contractors, suppliers, University partners, external researchers, visitors, and others who access or may have access to University information or technology.

2.3.2 Technologies or services used to access or process University information assets with applicability to anyone within the University.

2.3.3 Information assets processed in relation to any University function, including by, for, or with external parties.

2.3.4 Information assets that are stored by the University or an external service provider on behalf of the University.

2.3.5 Information that is transferred from and/or to the University for a functional purpose.

2.3.6 Third-party, public, civic, or other information that the University is storing, curating, or using on behalf of another party.

2.4 This Policy and the Framework apply irrespective of the location from which University information is accessed. As the University operates internationally and through arrangements with partners in other jurisdictions, the remit of the Policy and Framework shall include such overseas campuses and international activities. It shall pay due regard to non-UK legislation that might be applicable.

3. Policy Statement

3.1 The University is committed to preserving the confidentiality, integrity, and availability of all its key information assets to maintain its competitive edge, legal and contractual compliance and reputation. Key information assets are those that have some value either to the University, a department, or a user such that if it was lost/inaccessible or inaccurate, it would be difficult to replace without cost, skill, time or resources. This Policy and the Framework (comprising this Policy, supporting policies, standards and procedures and University governance relevant to information security) shall be enabling mechanisms for information sharing and for reducing information-related risk to acceptable levels, in line with risk appetite.

4. Policy

4.1 All persons within the scope of the Policy must protect data according to the provisions below:

4.2 **Training**: Users will be provided with regular and continuous mandatory information security awareness training, which will include nor be limited to: phishing simulation, guidance and specialist advice regarding information security risks, behaviours, expectations, and best practices. For the purpose of this policy, "regular" is defined as occurring at least once every twelve months. Compliance with this training is essential, and failure to complete it may result in restricted access to information systems and potential disciplinary actions.

4.3 **Information Asset Owner**: the University shall identify Information Asset Owners (IAOs) who are responsible for the management and processing of personal data held by the University. Heads of Professional Services, Colleges, Schools and other Heads of Business Units will be considered University Information Asset Owners . IAOs will ensure, with the support of the Information Compliance Team, that the Information Asset Register (IAR) and all other records of processing activities (ROPA), as required by GDPR Article 30, are wholly adequate and kept up-to date, and can be made available to the regulator, the Information Commissioner's Office (ICO) on request.

4.4 **Information Asset Register**: the University shall maintain an Information Asset Register recording the processing of all personal data by the University. The purpose of this register is to document information about what personal data is processed, the reason for processing, categories of data processed, where data is stored, how it is protected and what retention periods apply as well as identifying which individual or team is responsible for that data processing (the 'data owners').

4.5 A **Data Privacy Impact Assessment** (DPIA) must be carried out on all processes, technology, services and facilities relating to the processing of personal data, at the point they are introduced or changed. This must be carried out by the relevant Information Asset Owner (IAO) or responsible officer and be signed off by the Data Protection Officer (DPO). The aim of this assessment is to identify the value of information handled, its sensitivity, potential threats and weaknesses associated with the handling of information, system and its environment, technical architecture, regulatory compliance, supplier compliance with University requirements, and the appropriateness of security controls in place or planned. The key objective of this risk-based approach is to make informed decisions about how to manage and mitigate these risks effectively. Periodic review may be necessary to take into account changes to technology, legislation, and business requirements.

4.6 **Information Technology Due Diligence**: all information technology (IT) systems, hardware, services, suppliers and vendors must undergo a thorough due diligence process before their acquisition and integration into the University's infrastructure. This process includes, but is not limited to evaluating potential risks associated with the IT system or service, including information security risks, privacy risks, and compliance risks; vendor evaluation; contractual obligations; and cyber assurance. ISS has developed a set of thorough **technical requirements** to support all ICT purchasing activities across the University. IT procurement guidelines can be found on the ISS SharePoint site. Sign-off on the technical due diligence process is provided by the University Technical Design Authority owned by ISS.

4.7 **Risk Management**: information risks related to implementing this Policy shall be assessed using the University risk management approach defined in the Risk Management Policy. Privacy risks will be managed by the Data Protection Officer. Information risks outside of risk appetite will be notified to the University's Senior Information Risk Owner (SIRO) as defined in paragraph 6.3 of this Policy).

4.8 **Risk Acceptance**: The Senior Information Risk Owner has the authority to accept information security, privacy, and compliance risks for the University and in doing so will be guided by the wider risk appetites set by the University.

4.9 **Data Classification**: Information assets must be identified and classified into levels based on their sensitivity and risk of harm if the data were to be lost, changed, or disclosed. The University manages and produces information that is Public, Internal, Confidential and Highly Confidential in nature as defined in the Information Classification Policy.

4.10 **Data Security**: All information assets must be secured in line with the Information Classification Policy and must be used following the guidelines provided in the IT - Acceptable Use Policy and technical standards. Any security controls which are implemented must be developed and maintained in line with the findings of the relevant assessment (see 4.5 above). Controls for personal data processing must be proportionate to the risk of processing and the categories of personal data.

4.11 **Compliance**: All processes, technology, services, and facilities must be protected through appropriate information security controls in accordance with laws and regulations applicable to the University's operations and other requirements additionally imposed by any relevant contract terms.

4.12 **Information security incidents** must be identified, contained, remediated, investigated, and reported in accordance with the Incident Management Policy.

4.13 **Availability**: Back-up and disaster recovery plans, processes, and technology must be in place, and regularly tested, to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.

4.14 **Transnational Education Partners** are required to manage and own their cyber security posture. TNE partners shall undertake an annual information security penetration test together with a self-assessment security posture review to ensure awareness of strengths and weaknesses regarding security controls and culture. These requirements will form part of contractual obligations and as a condition for access to University resources in London. Cyber security posture for TNE partners will be reviewed annually or at the point contracts are introduced or renewed. TNE partners can decide whatever model or framework works best for them e.g. CIS controls, Cyber Assessment Framework, Cyber Essentials, ISO27001, or using internal risk assessments.

5. Framework

5.1 The University's information security is managed through the Framework shown on the next page in Figure 1 which comprises: (i) this Policy, (ii) Supporting policies, (iii) Standards and (iv) Procedures, alongside supporting governance processes. This Framework provides a flexible and effective platform upon which the University's information security objectives shall be met.
Examples of governance processes include the University risk management with operational and strategic risk registers, ISS cyber risk management board, Information governance advisory group, boards and decision-making groups.

5.2 Standards specify measurable requirements for compliance with University policies and applicable regulations and laws.

5.3 Standards must be considered as the minimum baseline requirements for information security.

5.4 Procedures are detailed plans to accomplish specific tasks or deliver services to meet the needs of the community while satisfying the requirements of applicable standards and policies. Developed and maintained by expert practitioners.

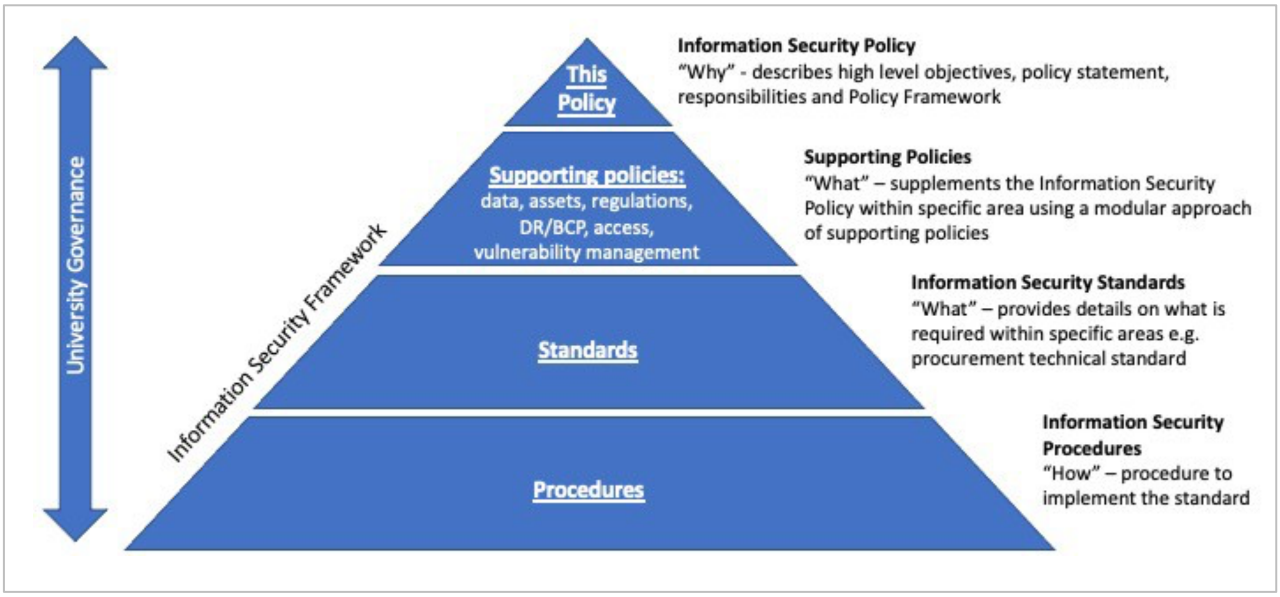
University Governance
Information Security Framework
This Policy
Supporting policies:
data, assets, regulations, DR/BCP, access, vulnerability management
Standards
Procedures
Information Security Policy
"Why" - describes high level objectives, policy statement, responsibilities and Policy Framework
Supporting Policies
"What" – supplements the Information Security Policy within specific area using a modular approach of supporting policies
Information Security Standards
"What" – provides details on what is required within specific areas e.g. procurement technical standard
Information Security Procedures
"How" – procedure to implement the standard

Figure 1: Information security framework

Information security framework diagram shows a hierarchy pyramid of 4 layers presented in the following order top to bottom. The entire hierarchy is covered by university governance.

6. Responsibilities

6.1 The **Court of Governors** is ultimately responsible for ensuring that the University meets its legal obligations.

6.2 **Overall responsibility and accountability** for this policy lies with the University's Senior Information Risk Owner (SIRO). SIRO may delegate specific or individual responsibilities to other roles within the University as they may deem appropriate; championing information risk management and assurance; championing a culture of security awareness among colleagues and students. SIRO has authority for risk acceptance as noted in paragraph 4.7. The SIRO promotes information security at senior level.

6.3 The **University Secretary and Chief Operating Officer** (USCOO), who is a member of the University Executive Board (UEB), has the role of SIRO.

6.4 **All users** of University information (as defined in paragraph 2.3.1 of the Policy) are responsible for:

- Undertaking mandatory training and awareness activities provided by the University to support compliance with this Policy and Framework.
- Taking all necessary steps to ensure that data are handled and processed in line with this Policy and no breaches of information security result from their actions.
- Reporting all suspected information security breaches or incidents promptly so that appropriate action can be taken to minimise harm.
- Only using systems and information for the purposes authorised.
- Only accessing systems and information for which they are authorised.
- Protecting information from unauthorised access, disclosure, modification, destruction or interference.
- Assisting in protecting University systems as far as reasonably possible from external threat e.g. phishing attempts and hacking attempts

- Complying with the requirements of this Policy and Framework. Failure to do so may result in the withdrawal of access to University information assets and technology. Serious breaches of this Policy and Framework will be dealt in accordance with paragraph 7.1 of the Policy.

6.5 **Heads of Schools, Heads of Colleges, Directors of Professional Services, and other Heads/Directors/CEO of Business Units including but not limited to Graduate School, Research and Knowledge Exchange Office, Business Engagement, Transnational Education, CETI, Student Union, and Transnational Education Partners** are responsible for implementing this Policy and Framework within their business areas and for adherence to the Policy and Framework by colleagues within their business areas. This includes:-

- Assigning generic and specific responsibilities for information security management.
- Managing access rights for information assets and systems within their area of responsibility to ensure that users of University information (as defined in paragraph 2.3.1 of the Policy) have access only to such confidential information as is necessary for them to fulfil their duties.
- Ensuring that all colleagues in their business areas undertake relevant training provided by the University and are aware of their accountability for information security.
- Ensuring that colleagues responsible for any locally managed specialist IT services approved by the Director of ISS adhere to the Cyber Essentials standard, University technical standards and to the University's IT Policies including IT Asset Management Policy, IT Administrator Policy, Patching Policy and liaise with colleagues in Information Systems and Support (ISS) to put in place relevant IT security controls where relevant.
- Ensuring that all colleagues involved in the development of projects, initiatives, studies, research, surveys, processes, and systems (known from this point as an 'Initiative') are aware of the **DPIA Policy** and understand the circumstances in which a DPIA and risk assessment (see 4.5) should be undertaken.
- Ensuring that colleagues or teams leading an Initiative undertake a **DPIA** as part of the University data controller obligations to safeguard data.
- Ensuring that managers in their business areas sign off team working agreements and colleagues are aware of their responsibilities and accountabilities for remote working.
- Ensuring that colleagues in their business areas follow this policy for the use of Generative AI (GenAI) for the safe, compliant and ethical use of GenAI.
- Ensuring that managers in their business areas comply with the records management policy for systems containing records.
- Ensuring that managers, academic supervisors and researchers in their business areas comply with research data management policies for managing research data.
- Ensuring that information security controls for each system under their control are documented.
- Ensuring that access to systems is limited only to those roles requiring access.
- Ensuring that where they cease using a third party hosted application that any data held by the supplier on behalf of the University is either securely destroyed by

the supplier or returned to the University.

6.6 **The Information Compliance Manager** is responsible for:

- Delivering the role of named Data Protection Officer and Freedom of Information Officer.
- Providing advice and guidance to colleagues and managers at all levels on all related data protection legislation
- Developing and managing organisational policies and procedures to ensure ongoing compliance with Data Protection and Freedom of Information legislation.
- For overseeing and reviewing the implementation of the **DPIA** Policy and must be consulted in relation to any DPIA's undertaken in accordance with the policy's requirements.
- Liaison with the Information Commissioner's Office on data protection matters, including the reporting of data breaches.

6.7 **The Head of Cyber Security,** (Information Systems and Support) is responsible for:

- Leading on Cyber Security and providing expert advice in proactively managing all aspects of the University's data and systems.
- Developing and maintaining a Cyber Security framework, encompassing architecture, standards and operational processes.
- Managing the Cyber Security team.

6.8 **The Director of Finance** is responsible for the University's compliance with the Payment Card Industry's Data Security Standard (PCI DSS). The University has a legal and contractual obligation to be compliant with PCI DSS. The University is committed to providing a secure environment for our users to protect against credit card fraud and data loss.

6.9 **The University Information Governance Advisory Group** (IGAG – ToR) is responsible for strategic oversight of Information Governance activities across the University. IGAG reports to the USCOO. Policies relating to information compliance, security and management are reviewed by the Group and recommended to the USCOO for final approval. The USCOO presents approved policies to the UEB for information.

6.10 **The ISS Cyber Security Risk Management Board** (CSRMB – ToR) is responsible for the execution of the development, prioritisation and progress monitoring of all cyber security related activities. CSRMB acts as a formal escalation point for cyber risks discovered during procurement for any new product or service or risks emerging from existing products or services.

6.11 **The Risk and Resilience Manager**, (Governance Team, Strategy, Performance and Planning) is responsible for developing, implementing and ensuring the effectiveness of the University-wide approach to business continuity and risk management.

6.12 **The Head of Organisational Development,** (People, Culture and Wellbeing) is responsible for providing access to appropriate Information Security training and for maintaining data on the extent to which colleagues have completed / are up-to-date with such training. Ensure mandatory training is undertaken.

6.13 **The Head of Cyber Security,** (Information Systems and Support) will contribute to Information Security training and education on cyber security by working closely with the HR lead for organisational development, taking the lead on all cyber security elements. The Head of Cyber Security is responsible for ensuring the content is up-to-date and relevant and determine what the refresher period would be to ensure training is up to date.

6.14 **The Director of Estates** is responsible for ensuring the security of all building premises within the University's estate, including implementing physical security measures and conducting regular security assessments. By fulfilling these responsibilities, the Director of Estate plays a crucial role in safeguarding the University's information security infrastructure and ensuring a safe environment for all members of the University community.

6.15 **The University Records and Archives team** is responsible for:

- The management, disposition and preservation of all University records (current, semi-current, archival), held in all formats in both University infrastructure and third-party storage.
- Developing and implementing organisational policies and procedures on records management and digital preservation practices.
- Providing guidance and training to colleagues and managers at all levels on record-keeping.

6.16 **The Director of Transnational Education** is responsible for implementing the contract clauses for cyber security assurance as defined in paragraph 4.14 of this Policy and managing the TNE partners compliance with cyber security assurance.

6.17 The Head of IT Infrastructure operations in ISS is accountable for the Business Continuity Management for all IT services controlled by ISS, ensuring they are documented and tested in line with best practice expectations.

6.18 The Head of IT Developments in ISS is responsible to lead the Technical Design Authority group to establish and adopt best practice technology standards that ensure accessible, resilient and safe IT environments that directly support the University’s ambitions.

7. Compliance

7.1 Failure to meet the requirements detailed within this Policy and the Framework in protecting University information (or that entrusted or us by a third party) puts the University at risk of reputational damage, financial penalty, breach of legal, contractual or regulatory requirements. It may also lead to restricted access to information systems and disciplinary action that will be dealt with under the appropriate disciplinary code or procedures. Additionally, where it is suspected that an offence has occurred under UK law, it may also be reported to the police or other appropriate authorities.

8. Review and Development

8.1 This University policy shall be reviewed and updated by ISS, and the relevant Governance Group on an annual basis. Other supporting policies shall be reviewed by the respective owners and committees according to their schedule of approval and review dates to ensure that they:

- Remain operationally fit for purpose.
- Are aligned to industry best practice.
- Support continued regulatory, contractual and legal compliance.

9. Supporting Policies

9.1 This Policy should be read in conjunction with other supporting policies. This Policy and supporting policies are reviewed and updated as necessary to maintain an effective Information Security Management System to meet the University's business needs and legal obligations.

9.2 Figure 2 below shows this Policy as the overarching information security policy at the top and supporting policies underneath. Supporting policies cover Data, IT assets, IT regulations, IT disaster recovery (DR) and business continuity planning (BCP), IT elevated access management, and vulnerability management policies.

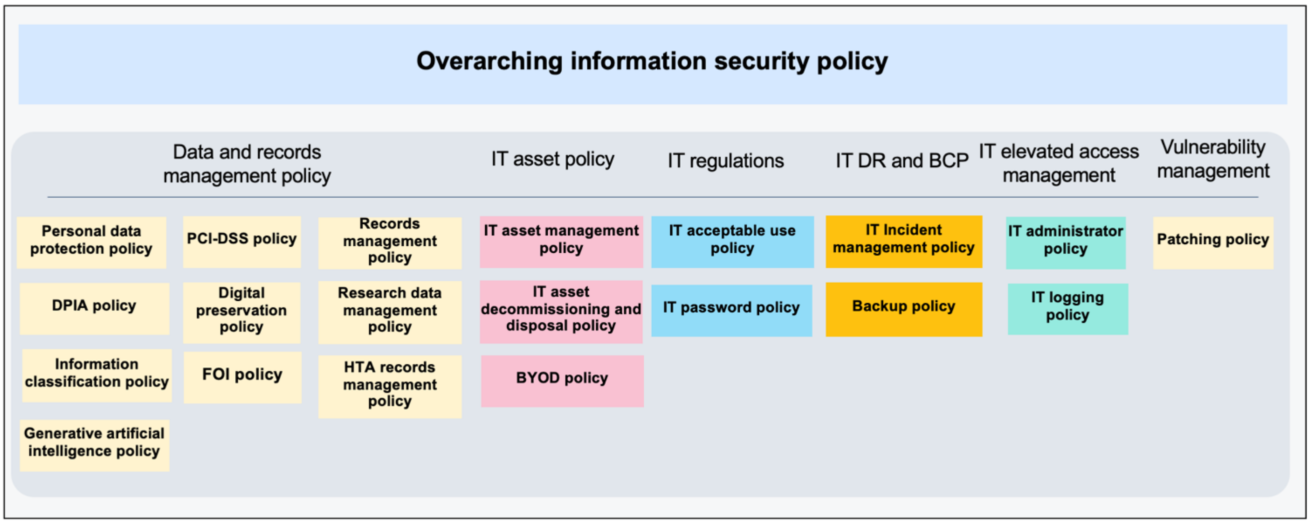
Overarching information security policy
Data and records management policy
IT asset policy
IT regulations
IT DR and BCP
IT elevated access management
Vulnerability management
Personal data protection policy
PCI-DSS policy
Records management policy
DPIA policy
Digital preservation policy
Research data management policy
Information classification policy
FOI policy
HTA records management policy
Generative artificial intelligence policy
IT asset management policy
IT asset decommissioning and disposal policy
BYOD policy
IT acceptable use policy
IT password policy
IT Incident management policy
Backup policy
IT administrator policy
IT logging policy
Patching policy

Figure 2: Information security policy and supporting policies

Figure 2 description. The above diagram shows the supporting policies covered by the following list:

- Data and record management policies – Personal data protection, DPIA, Information classification, Generative AI, PCI-DSS, Digital preservation, FOIs, Records management, Research data management, HTA records management
- IT asset policies – IT asset management, IT asset decommissioning and disposal, BYOD, Record management
- IT regulations – IT acceptable use, IT passwords
- IT DR and BCP policies – IT incident management, Backups
- IT elevated access management policies – IT administrator, IT logging
- Vulnerability management policies – Patching policy

10. Publishing Policies

We are committed to ensuring our websites and content is digitally accessible according to the Public Sector Bodies Accessibility Regulations (2018). This policy is published on the University website and can be requested in a range of formats e.g. Word, PDF, plain text, alternative formats such as large print or Braille.

11. Legal Requirements

11.1 Effective information security controls are essential for compliance within the UK and other relevant law in all jurisdictions in which the University operates. Legislation that places specific information security and record keeping obligations on organisations includes, but is not limited to:

- National Security Act 2023.

- National Security and Investment Act (NSI) 2022.
- Academic Technology Approval Scheme (ATAS).
- Import and Export Controls.
- UK General Data Protection Regulations.
- Data Protection Act 2018.
- Privacy and Electronic Communications Regulations 2003.
- Counter-terrorism and Security Act 2015.
- Computer Misuse Act 1990.
- Regulation of Investigatory Powers Act 2000.
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

11.2 All current UK Legislation is published at www.legislation.gov.uk

12. Further Help and Advice

For further information and advice about this policy and any aspect of information security contact:
IT Security cybersecurity@westminster.ac.uk