University VPN Policy University of Edinburgh

The University of Edinburgh provides Virtual Private Network (VPN) services to enable secure remote access to university resources. This policy outlines the acceptable use and security requirements for VPN services.

1. Purpose and Scope The VPN service allows authorized users to securely access university systems and data from off-campus locations. This policy applies to all users of university VPN services.
2. Eligibility VPN access is available to:
    - Current students enrolled in degree programs
    - Active staff members
    - Authorized contractors with valid agreements
    - Visiting researchers with appropriate permissions
3. Security Requirements All VPN users must comply with the following security requirements:
    - Use strong authentication methods
    - Keep VPN client software updated
    - Report security incidents immediately
    - Follow data handling procedures
4. User Responsibilities

Users of university VPN services must:

- Use VPN only for authorized university activities
- Maintain confidentiality of VPN credentials
- Report suspected security incidents immediately
- Comply with all university IT policies and procedures
- Accept that VPN usage may be monitored and logged

5. Prohibited Activities The following activities are strictly forbidden:

- Sharing VPN credentials with unauthorized persons
- Using VPN for illegal activities or copyright infringement
- Circumventing university network security controls
- Excessive bandwidth usage affecting service performance
- Accessing prohibited or inappropriate content

6. Compliance and Enforcement Violations of this policy may result in:

- Immediate suspension of VPN access
- Disciplinary action under university policies
- Legal action where appropriate
- Academic sanctions for students

7. Technical Requirements

VPN Client Software: - Must be the latest supported version - Regular updates required - Compatible with university infrastructure

Network Requirements: - Stable internet connection - Minimum bandwidth requirements - Firewall configuration compliance

8. Data Protection

When using VPN services: - All data transmission is encrypted - University data must be handled according to GDPR - Personal devices must meet security standards - Regular security assessments required

9. Support and Maintenance

VPN Support: - Available during business hours - Emergency support for critical issues - Regular maintenance windows scheduled - User training and documentation provided

Contact Information: - VPN Support: vpn-support@ed.ac.uk - IT Helpdesk: ithelpdesk@ed.ac.uk - Emergency: +44 131 651 5151