1. Introduction

This Acceptable Use Policy ("AUP") sets out the rules governing the use of services provided by Oakford Internet Services ("OIS", "we", "our", "us").

It is designed to:

- Ensure lawful, secure, and fair use of our services
- Protect the integrity, availability, and performance of our network
- Safeguard our customers, users, and reputation.

By using OIS services, you agree to comply with this AUP.

Users should read this policy alongside other OIS and other suppliers policies.

User organisations should implement their own AUPs to ensure all users of the Services understand the conditions under which the OIS Services may be used.

2. Scope

This policy applies to:

- All customers, users, and organisations using OIS services / infrastructure
- Any individual accessing services through a customer account
- All forms of usage, including internet access, email, hosting, cloud, and managed services.

Customers are responsible for:

- All activity conducted via their account(s)
- Ensuring authorised access only
- Maintaining appropriate internal policies for their users.

3. General Principles

Users must:

- Comply with all applicable UK laws and regulations
- Use services responsibly and ethically
- Avoid actions that may harm OIS, its customers, or third parties.

Use must not:

- Disrupt service performance or availability
- Compromise security or data integrity
- Damage the reputation of OIS.

4. Prohibited Activities

Users must not use OIS services to:

4.1 Illegal or Harmful Content

Access, create, store, or distribute content that:

- Is illegal under UK law

- Includes child exploitation material
- Promotes violence, terrorism, or criminal activity
- Incites hatred, discrimination, or harassment
- Is defamatory, obscene, or offensive.

4.2 Security Violations

Users must not:

- Attempt unauthorised access to systems, accounts, or networks
- Conduct vulnerability scanning, penetration testing, or probing without explicit written consent
- Intercept or monitor network traffic without authorisation
- Use spoofing, impersonation, or phishing techniques
- Introduce malware, viruses, or malicious code.

4.3 Network Abuse

Users must not:

- Launch or participate in Denial-of-Service (DoS/DDoS) attacks
- Generate excessive traffic that degrades network performance
- Operate botnets or distribute malware
- Send or facilitate unsolicited bulk communications (spam)
- Engage in crypto-mining or similar resource-intensive activities without approval.

4.4 Data & Privacy Violations

Users must not:

- Process or share personal data unlawfully
- Breach UK GDPR or data protection legislation
- Disclose confidential or proprietary information without authorisation.

This includes (but is not limited to):

- Personal data
- Financial information
- Credentials and access codes
- Business-sensitive information.

4.5 Intellectual Property Violations

Users must not:

- Upload, download, or distribute copyrighted material without permission
- Use OIS services for software piracy or licence abuse.

4.6 Misuse of Services

Users must not:

- Use services to run unauthorised commercial activities
- Misrepresent OIS or their affiliation with OIS
- Use services in a way that could damage OIS's reputation
- Engage in fraudulent or deceptive practices.

4.7 Automation & Abuse of Systems

Users must not:

- Use bots, scripts, or automated tools to access services in a way that causes disruption
- Perform data scraping or harvesting without permission
- Circumvent usage controls or rate limits.

5. Acceptable Use Expectations

Customers and users must:

- Keep passwords and access credentials secure
- Maintain appropriate device security (e.g. patching, antivirus, encryption)
- Ensure only authorised users access the services
- Report suspected security incidents promptly.

6. Monitoring and Enforcement

OIS may:

- Monitor network and service usage to ensure compliance
- Investigate suspected breaches of this AUP
- Share relevant information with customers, regulators, or law enforcement where required.

Where a breach is identified, OIS reserves the right to:

- Issue warnings
- Suspend or restrict services
- Terminate services immediately (in serious cases).

7. Reporting Abuse and Security Issues

Suspected breaches or security concerns should be reported immediately to:

Service Desk: support@oakfordis.com

Abuse: abuse@oakfordis.com

Users should:

- Preserve relevant evidence where possible
- Follow their organisation's internal escalation procedures.

8. Customer Responsibilities

Customer organisations must:

- Ensure their users are aware of and comply with this AUP
- Implement appropriate internal acceptable use policies
- Cooperate with OIS investigations where necessary
- Indemnify OIS against claims arising from misuse of services.

9. Fair Use and Network Integrity

OIS services are provided on a fair-use basis.

We reserve the right to:

- Manage traffic to maintain service quality
- Apply controls to prevent abuse or network degradation.

10. Policy Updates

We may update this AUP from time to time to reflect:

- Changes in law or regulation
- Emerging security threats
- Service or technology changes.

The latest version will always be available on request or via our website.

Continued use of OIS services constitutes acceptance of the current version.

11. Related Policies

This AUP should be read alongside:

- Terms and Conditions
- Privacy Policy
- Data Protection Policy
- Information Security Policy (where applicable).