



ACCEPTABLE USAGE POLICY

1. Purpose

This Acceptable Use Policy defines the prohibited use of Central Technology's systems, networks, and data to ensure:

- Protection of information assets
- Compliance with applicable legislation (UK GDPR, Data Protection Act 2018 Computer Misuse Act 1990)
- Alignment with ISO/IEC 27001:2022 information security controls

2. Scope

This policy applies to:

- All customers, contractors, and third parties
- All systems, networks, applications, and devices (including BYOD where authorised)
- All data stored, processed, or transmitted via Central Technology's services

3. User Responsibilities

Users must:

- Use systems **lawfully, securely, and for authorised business purposes**
- Comply with this policy and all related information security policies
- Ensure devices and credentials are protected (e.g. strong passwords and MFA where applicable)
- Report **security incidents, suspicious activity, or policy breaches immediately**
- Ensure and third-party users under their control comply with this policy

4. Acceptable Use

Permitted use includes:

- Accessing systems and data required for authorised business activities
- Limited personal use where it does **not**:
 - Affect performance or delivery
 - Introduce security risks
 - Break any applicable laws or policies



5. Prohibited Use

Users must not:

5.1 Security & Network Misuse

- Attempt unauthorised access to systems, networks or data
- Conduct vulnerability scanning, penetration testing, or probing with explicit approval from Central Technology
- Launch or participate in:
 - Denial-of-service (DoS/DDoS) attacks
 - “Mailbombing” or network flooding
- Introduce malware (viruses, ransomware, malicious scripts)
- Circumvent authentication or security controls

5.2 Data & Information Misuse

- Access, copy, or share data without authorisation
- Process personal data outside approved systems
- Store company or customer data on unauthorised platforms
- Delete or alter data without permission

5.3 Illegal or Inappropriate Content

Users must not create, store, transmit, or access:

- Illegal material (including content prohibited under UK law)
- Offensive, abusive, defamatory, or discriminatory content
- Content which promotes criminal or unlawful behaviour

5.4 Email & Internet Misuse

- Send unsolicited bulk mail (spam)
- Run open mail relays or facilitate spam distribution
- Phishing, spoofing or impersonation

5.5 Intellectual Property Violations

Users must not:

- Use or distribute copyrighted material without permissions
- Infringe trademarks or proprietary rights
- Use unlicensed software



5.6 Privacy Violations

Users must not:

- Monitor or intercept communications without authority
- Access or disclose personal or confidential data
- Forge, conceal, or manipulate identity (e.g. spoofing email headers)

6. Information Security Requirements

Users must:

- Follow password and authentication policies (including MFA where required)
- Ensure devices are securely configured and updated
- Use approved systems (e.g. corporate email, SharePoint, secure file transfer)
- Avoid use of unauthorised software or shadow IT

7. Monitoring & Compliance

Central Technology:

- May monitor system and network usage for:
 - Security
 - Compliance
 - Service performance
- Will investigate all reported or suspected violations

8. Incident Management

Users must:

- Report incidents immediately (e.g. security breach, virus, data loss etc.)
- Cooperate with any investigations

Central Technology will:

- Investigate all incidents
- Escalate to the appropriate authorities/ law enforcement where required

9. Enforcement & Sanctions

Breaches of this policy may result in:

- Suspension of Services
- Restriction of access
- Contract termination
- Civil or criminal proceedings



10. Third-Party & Customer Responsibility

Customer must:

- Ensure all users of their services comply with this policy
- Accept liability for misuse by authorised users

11. Policy Governance

- Reviewed annually or upon any significant change
- Approved by senior management
- Available on request and via www.ct.co.uk

12. Complaints & Reporting

All suspected breaches or concerns must be reported to Central Technology

General Provisions

This policy provides guidance on acceptable and unacceptable use; however, it is not exhaustive.

Any use of Central Technology systems, networks, or services that is deemed illegal, unethical, or otherwise unacceptable, whether explicitly stated in this policy or not, will be fully investigated.

Central Technology will act in accordance with applicable legislation and may seek and follow guidance from relevant independent industry bodies where appropriate.

The decision of Central Technology regarding any matter relating to this policy shall be final.

