The 16-Section AUP Checklist for SMEs

A practical reference for building or auditing your Acceptable Use Policy under ISO 27001 Control 5.10

By Alan Parker, ISO 27001 Consultant, Iseo Blue Limited

Use this checklist when writing a new Acceptable Use Policy or auditing an existing one. If your AUP covers each section meaningfully (not just with a heading and one line of filler), you're in good shape for both the control and the audit.

For most SMEs, the AUP is best kept to 6-10 pages. Long enough to cover the ground; short enough that people actually read it.

Core sections

(every AUP needs these)

☐ **1. Purpose and Scope**
What the policy is for. Who it applies to (employees, contractors, third parties, visitors). What assets it covers (company systems, BYOD, cloud services, physical premises). Applies wherever company information is handled, not just on company premises.

☐ **2. Roles and Responsibilities**
Who owns the policy. Who enforces it. Who staff contact with questions. Brief; references your wider roles documentation.

☐ **3. General Principles of Acceptable Use**
The headline behaviours. Legitimate business use. No illegal or harmful activity. Protect information appropriately. Follow related policies.

☐ **4. Use of Company Systems and Devices**
Operational rules for laptops, desktops, mobile devices, and company-issued hardware. Software updates. No unauthorised installs. No disabling security tools. Lock screens. Report loss or theft promptly.

☐ **5. Email and Communications**
Appropriate use of company email. No personal email for company business. Phishing awareness. No forwarding company information to personal accounts. Professional conduct. Note that email is monitored.

☐ **6. Internet and Web Use**
Acceptable browsing. No illegal or inappropriate content. Caution around uploading company information to web services. Activity may be monitored.

☐ **7. Information Handling**
How to handle information by classification (where to store, how to transfer, how to dispose of). Links to your classification scheme under Control 5.12.

☐ **8. Passwords and Authentication**
Keep passwords secret. No shared accounts. Use MFA where available. Report suspected compromise. Or reference a separate Password Policy if you have one.

Modern essentials

(often missed)

☐ **9. Working Outside the Office**
Securing devices when remote. Approved networks. Physical security in public spaces (overheard calls, screen privacy). Care with paper documents.

☐ **10. Personal Use**
Honest acknowledgement that some personal use is acceptable. Clear limits (occasional, reasonable, not damaging). No expectation of privacy on company systems. Pretending it doesn't happen rarely works.

☐ **11. Use of AI Tools (2026 essential)**
Which AI tools are approved. What information can and cannot be shared. Awareness that prompts and outputs may be stored by the provider. Professional responsibility for AI-generated outputs.

☐ **12. Social Media**
Representing the company appropriately. No disclosure of confidential information. Line between personal opinion and company position. Awareness of social engineering risk.

☐ **13. Bring Your Own Device (BYOD)**
If personal devices access company information, the conditions sit here. Device security requirements. Acceptance that company data on the device may be remotely wiped.

Governance and administration

☐ **14. Monitoring and Privacy**
Honest disclosure that company systems may be monitored. What data is retained. Legal protection language without going into operational detail.

☐ **15. Reporting Issues**
How and where to report suspected incidents, policy violations, or security concerns. Who to contact. Protections for good-faith reporting.

☐ **16. Consequences of Non-Compliance**
Brief but clear. References (does not reproduce) the disciplinary process under Control 6.4. The point is seriousness, not threat.

Quick audit-readiness check

Even with all 16 sections covered, the AUP only works if these are also true:

☐ The policy is approved, dated, version-controlled, and has a named owner
☐ Staff have read and acknowledged it (captured in an auditable system, not just “it's on SharePoint”)
☐ Acknowledgement is repeated annually or when the policy materially changes
☐ The AUP is referenced by your awareness training
☐ Supporting procedures exist for the activities the AUP describes (data transfer, lost device, suspicious email, etc.)
☐ The AUP applies to contractors and third parties where they access your information

If you can tick all six of these alongside the 16 sections, you're satisfying Control 5.10 properly and will pass audit on this one.

Need help going further?

The full **Iseo Blue ISO 27001 Toolkit** includes a ready-to-edit Acceptable Use Policy template alongside the wider ISMS document set, all written for SME use.

https://iseoblue.com/iso-27001/iso-27001-toolkit

If you'd rather talk through how to right-size your AUP for your specific business, the **free 30-minute consultation** is genuinely free and genuinely 30 minutes.

https://iseoblue.com/iso-27001/consultancy

iseo blue