Acceptable Use Policy Template for UK Businesses

What an Acceptable Use Policy Is

- Definition of an Acceptable Use Policy (AUP)
- Reasons for having an AUP: To be clear, fair, and to protect those who are using computers
- How an AUP aids employees in understanding what is expected of them
- An AUP protects businesses from avoidable risk
- What is an AUP not (e.g., it is not to be used as a means of surveillance or enforcement of the law)

Who This Policy Is For / Who It's Not For

- UK-based businesses having 1-250 employees
- Businesses with staff working in office and/or remote capacities and having a hybrid workforce.
- Persons filling the following roles: Directors; Human Resource Managers; Operations Managers.
- Non-technical staff who use company's IT systems on a daily basis.

Who this policy is not for

- Large, complex organisations with multiple regulations to comply with.
- Independent Contractors bound by their own legal or contractual agreements.
- Organisations that need to use specific language in their sector.

Why Every UK Business Needs an Acceptable Use Policy

- Minimise risk to your organisation from cyber security related to every day activities.
- Support UK GDPR and the Data Protection Act 2018 (high level).
- Provide clarification and consistency in HR management and rules.
- Support fair processes of discipline that are aligned with ACAS guidance.
- Protect the organisation from the consequences of incidents, audits or disputes.
- Why relying on trust is not an effective method of control.

How to Implement and Enforce the Policy

- Identify who is responsible for the policy (HR, Director, IT).
- Plan how to distribute the policy to all employees.
- Prepare the policy so that it is easy to understand and find.
- Train and inform employees (light touch or practical).
- Enforce the policy in a consistent and fair way.

- Use the policy as an attachment to contracts and staff handbooks (high level).

1. Purpose and scope

This policy describes the proper and responsible use of Company information systems, devices and data by all employees, contractors, temporary workers. This policy applies to all employees and anyone who uses Company-owned equipment or accesses Company systems.

2. Devices covered

There are two types of devices included under this policy:

- Company-owned equipment: Laptops, desktops, phones, tablets, printers, USB sticks, etc.
- Personal devices: Your own phone, laptop, or tablet that you use for work (see section 9 for the BYOD policy).

3. Acceptable use

All business-related activities performed using your device are acceptable.

There are certain types of personal use that are acceptable. These types of personal use can be used only while on break or not during your core working hours.

Examples of acceptable personal use:

- Checking your personal e-mail accounts.

- Looking up the news or weather.
- Making an appointment with your doctor.
- Searching the Internet for 10 each to 15 minutes for personal purposes.

Personal use of Company-owned systems and devices, and the Internet, should not detract from your performance at work or consume more than a reasonable amount of bandwidth.

4. Prohibited use

You must not:

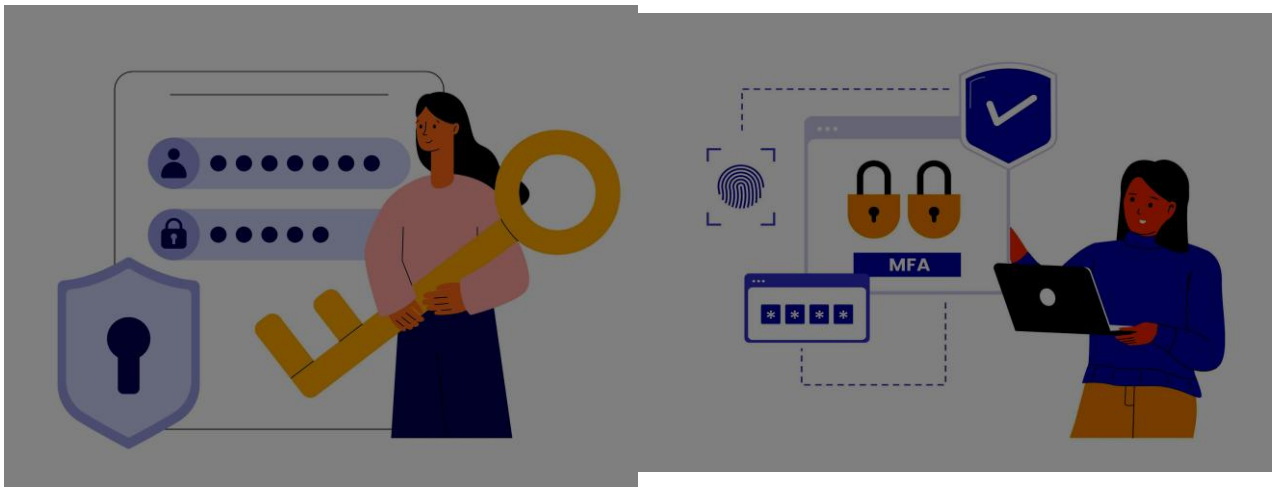
- Access / download / store / share anything illegal (including copyright infringement)
- Visit sites or use services that are pornographic, violent, hate speech or discriminatory in nature
- Download or install any software unless given express permission
- Share your accounts and/or passwords with anyone else
- Use the company system for any form of harassment/bullying/discriminatory purpose
- Send out spam
- Attempt to circumvent security controls

5. Email, internet and cloud services

- All work-related email correspondence must use your company email account.
- Do not use personal email accounts to conduct business on behalf of the company without approval to do so.
- If you have an email you would like us not to read (genuinely private), please put the word "private personal" in the email subject line (we seldom read personal emails).
- Cloud services (Microsoft 365, Google Workspace, Dropbox, etc.) must only be used with your company account.

6. Passwords and account security

- Select your passwords to be strong and not shared with anyone, e.g. a minimum of 12 characters with a mixture of numbers/letters/special characters.
- Change your passwords every 90 days or if requested.
- Never share your passwords.
- Lock your screen when you leave your computer.
- Whenever available, enable multi-factor authentication (MFA) where you can.



7. Data protection and confidentiality

- All customer and co-worker personal data must be treated as confidential.
- Access only the data you require for your work.
- Do not share any data outside of the company unless you have permission to do so.
- Report any accidental data disclosure immediately (see Section 11).

8. Software installation and licensing

- You will only install software approved by IT/Operations.
- All software must have the appropriate licensing.
- All operating systems and anti-virus products must be kept current on their respective support release schedules.

9) Remote Working and Home Office Use

- When connecting to a company system from outside of the office, you should use a VPN to securely connect to company systems.
- Company devices should reside in a secure location within the home.
- You should never leave a company owned device unattended while in a public place.
- Company policies with regard to security are the same while working from home as they are in the office.

10) Monitoring and Privacy Notice (UK-Compliant)

We monitor all systems that you connect to (email, internet usage, device logs, login time) in order to:

- Protect Company Data/Systems
- Prevent Company Security Incidents

- Ensure Company Compliance to Company Policy

All monitoring is proportional and to the degree that is necessary. We do not monitor an employee's email account for private messages that are marked as "Private-Personal".

Advice on Customisation

- Be sure to insert [Company Name] and contact info.
- Make sure you personalise with your logo and header/footer (assuming you have one).
- If applicable, have stricter language for regulated industries (i.e. “No personal use of company email without prior written consent”).
- Add specific tools you use to communicate with users (i.e. Slack, Teams, Zoom).
- For BYOD: Add the following statement: “We may remotely erase company data from the device if it is lost.”
- Link to full privacy notice and disciplinary policy.

Mistakes to Avoid

- Do not make it too long or legalistic → staff will not read.
- Do not forget to include monitoring → ICO fines and employee complaints.
- No BYOD rules → Data leaks on personal mobile devices.
- No record of staff sign-offs → Difficult to prove staff have been made aware of rules.
- Do not ever review it → Becomes obsolete after software changes or changes in mode of work, i.e., work remotely.
- Do not use threatening language → Damages trust and fairness

FAQs

➢ **Is a legally required Acceptable Use Policy in the UK?**

An Acceptable Use Policy is not legally required in the UK; however, it is highly recommended by the Information Commissioner's Office, The Advisory, Conciliation and Arbitration Service and Cyber Insurance Providers. Additionally, having a policy demonstrates accountability under the UK GDPR Article 5 (2) and provides a defence against any claim that could be made against you.

➢ **Can employers monitor their employees?**

Yes, as long as you are open about doing so, you have a lawful basis (usually legitimate interests), you are being proportionate in your actions, and you have notified your employees in advance of the monitoring of their activity (through this policy and privacy notice). You must carry out a Data Protection Impact Assessment for any monitoring that may be considered intrusive.

➢ **How often do I need to review the Acceptable Use Policy?**

You must review your Acceptable Use Policy no less than every 12 months or when there is a major change (i.e. introduction of new software, introduction of hybrid-working policy, update to ICO guidance).

- **Do the same rules apply when working remotely?**

Yes. The same rules apply regardless of whether you are working in an office, at home or on the go.

- **Can I use my personal device (BYOD) to work?**

Provided you comply with the requirements of Section 9, you can use your personal device (BYOD) to do your job. We recommend that you create a separate BYOD policy if you have a significant number of staff using personal devices.

About This Guide

UK-based IT Support and Cybersecurity Firm **Computer Support Centre** has compiled the following safe use of IT systems (Acceptable Use Policy) to assist directors, HR managers and employees in understanding their obligations under this company policy to ensure that company systems are used appropriately, equitably and legally. Many companies struggle with having an AUP that is either too technical, too legal or taken directly from a template and the staff is unable to read or comply with the terms of the policy. This guide was developed with the intent of sharing real experiences that **Computer Support Centre** has encountered while providing IT Support to UK businesses, remote teams and businesses utilising a hybrid working arrangement.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

An Acceptable Use Policy is intended to set expectations for behaviour, provide a framework for protecting the interests of the organisation, and assist staff to be able to properly and safely utilise technology.

In the UK, an up-to-date and comprehensive Acceptable Use Policy provides your organisation with improved security and decreased chances of misunderstanding, and helps demonstrate uncompromised professional management of your organisation in compliance with UK employment and data protection laws. An Acceptable Use Policy should be created in plain English with clear and easy implementation; when done so, the Acceptable Use Policy becomes a valuable reference instead of a document that people will ignore.

This guide and template can be used to create an Acceptable Use Policy for your organisation that can be distributed to staff and reviewed on an ongoing basis as the organisation and the technology used/available to staff are continually changing.

A well-written Acceptable Use Policy provides staff with a practical tool for supporting staff, safeguarding organisational data, and enhancing the vitality of the organisation.