IT & Acceptable Use Policy

Policy · UK · Updated 2026-07-23 · Square brackets are placeholders to replace with your own details.

An IT and acceptable use policy is the written set of rules for how staff use your organisation's systems, devices, email, and internet access — what is allowed, what is banned, and what to do when something goes wrong. It is the document you reach for when an account is compromised, a laptop goes missing, or someone's use of company systems becomes a problem.

Most security incidents start with ordinary user behaviour: a reused password, a phishing link, work files copied to a personal account. A short, trained acceptable use policy is the cheapest security control a small business can deploy — and without one, disciplining misuse is an uphill argument.

This template gives you the full policy: acceptable and unacceptable use, password and device security, personal use and monitoring, and an incident reporting procedure.

Purpose and scope

This policy sets the rules for using [Your company]'s IT systems: computers, phones, email, internet access, software, and the cloud services we provide, including [list main systems]. It applies to all employees, contractors, and anyone else given access, whether working on site or remotely.

Its purpose is to protect our systems, our data, and the people whose personal information we hold — and to make sure nobody is disciplined for breaking a rule they were never told about.

Policy statement

[Your company] provides IT systems so people can do their jobs. We expect everyone to use them lawfully, securely, and professionally. Reasonable personal use is permitted within the limits below, but the systems remain company property and business needs come first.

Breaches are dealt with under the disciplinary policy and, where personal data is involved, under our data protection procedures.

Responsibilities

- Policy owner ([name/role]): keeps this policy current, approves exceptions in writing, and reviews incidents.
- IT lead ([name/role or provider]): manages accounts and access rights, applies security updates, and responds to reported incidents.
- Managers: confirm their team has read this policy, and request access changes when people join, change roles, or leave.
- All users: follow the rules, complete required training, and report anything suspicious without delay.

Acceptable use

- Work under your own named account — never use someone else's login, and never lend yours.

- Use only software and cloud services approved by [IT lead/role]; ask before installing anything new.
- Store work files in [approved location, e.g. the company drive], not on desktops, USB sticks, or personal cloud accounts.
- Lock your screen whenever you leave a device unattended, on site or at home.
- Keep business communication in company email and messaging so records stay in company systems.

Unacceptable use

- Sharing your password or credentials with anyone, including colleagues and managers.
- Accessing, storing, or sending material that is illegal, discriminatory, pornographic, or likely to harass or offend.
- Sending company or customer data to personal email accounts or personal storage.
- Attempting to access systems, records, or accounts you are not authorised to use — this can also be a criminal offence.
- Disabling security controls such as antivirus software, screen locks, or device encryption.
- Using company systems to run a personal business or for any other unlawful activity.

Passwords, devices and security basics

- Use a strong, unique password for every company account, and change it immediately if you suspect anyone else knows it.
- Turn on multi-factor authentication wherever [IT lead/role] has made it available.
- Treat unexpected messages asking for logins, payments, or urgent action as suspect — verify through a second channel before acting.
- Install security updates promptly; do not postpone them for more than [number] days.
- Report lost or stolen devices to [name/role] immediately, at any hour — speed limits the damage.

Personal use and monitoring

Reasonable personal use of email and the internet is allowed during breaks, provided it does not interfere with work, use significant resources, or involve anything listed as unacceptable use. Personal use is a privilege we can restrict for operational reasons.

[Your company] monitors its systems only to the extent needed for security, legal compliance, and operational management — currently [describe: spam filtering, web filtering logs, access logs]. We do not routinely read personal messages, and any targeted monitoring must be authorised by [senior role] and recorded. Full details are in our employee privacy notice; if what we monitor changes, we will tell you before the change takes effect.

Security incidents, records and review

Signed acknowledgments, training records, and the incident log are kept in [system/location]. This policy is reviewed [frequency, e.g. annually] and after any significant incident. Owner: [name/role]. Next review: [date].

1. Report suspected incidents — a clicked phishing link, a lost device, an email to the wrong recipient, unusual account activity — to [name/role] immediately. Nobody will be criticised for reporting an honest mistake quickly.
2. [Name/role] contains the incident: isolating devices, resetting credentials, and preserving evidence.
3. If personal data is involved, follow the data breach response procedure — notifiable breaches must reach the ICO within 72 hours of awareness.
4. Record the incident, its cause, and the fix in [log/system], and feed lessons back into training.

How to use this template

1. List the systems people actually use before editing — the policy should name real tools, not generic categories.
2. Agree the monitoring paragraph with whoever runs your IT, and check it matches your employee privacy notice exactly.
3. Decide your position on personal use and state it plainly — vague tolerance is where disputes start.
4. Fill every [bracketed placeholder], and name a real person for incident reports with a deputy for absences.
5. Collect a signed or digital acknowledgment from every user — an unacknowledged IT policy is hard to enforce.
6. Reissue and retrain whenever you adopt a major new system; do not just re-send the document.

Official guidance

› ICO — UK GDPR guidance and resources

› ICO — Report a breach