

BEFORE YOU START

Making this policy **your own**

This is a template acceptable use policy for a small business. It sets out how staff and visitors may use your network, computers and accounts, and tells them what is monitored. Fill in the blanks, remove what doesn't apply, and it becomes your policy.

- 1 You fill in every blank (a line like _____). The table below lists them.
- 2 You remove any clause marked **OPTIONAL** that doesn't fit your business, and renumber what's left.
- 3 You check the monitoring table (clause 12) matches what your systems actually record. If you aren't sure, ask whoever looks after your IT.
- 4 Someone with authority approves it on the policy pages, and you remove this page.
- 5 Everyone who signs in confirms they've read it, online or on the acknowledgement page.

THE BLANKS TO FILL IN

Where	What goes there
Front page	Your logo, your business's full name, who supplies your IT (if anyone), the version and date.
Clause 7.1	The kinds of website you block for everyone.
Clause 12.2	What is recorded, who can see it, how often you get reports and how long it's kept.
Clauses 13.2 and 14	Who staff contact about their data, and who they tell about a problem.
Clause 17.1	Who owns the policy.
Acknowledgement page	The address of your online acknowledgement form, if you have one.

This template is not legal advice

Cryptal Media Group Ltd. publishes this template for general information. We don't give legal, HR or employment advice, and using the template doesn't make us your adviser. You're responsible for the final policy and how you use it. Take your own legal or HR advice, particularly on monitoring and on how the policy fits your contracts of employment.

Cryptal Media Group Ltd.

Help setting up the filtering and monitoring this policy describes: networks@cryptalmedia.com

YOUR LOGO

POLICY

Acceptable use policy

Terms governing access to and use of the network,
computers and accounts of _____
by all users and devices, including notice of monitoring.

POLICY OWNER

IT PROVIDER

VERSION

DATE

ACCEPTABLE USE POLICY

Terms of use of **our network**

Summary

This summary is for convenience only. The numbered clauses that follow form the policy and take precedence.

- The Company's network and systems are provided for business purposes. Reasonable personal use, including reasonable use of social media, is permitted.
- Credentials must not be shared. Security controls, filtering and monitoring must not be circumvented.
- Use of the network is monitored as described in clause 12.
- Breach may result in restriction or withdrawal of network access or use of Company devices.

1 Purpose

- 1.1 This policy sets out the terms on which Users may access and use the Network and Company Systems, in order to protect the Company, its information, its customers and its Users, and to support compliance with applicable law.
- 1.2 This policy also gives notice to Users of the monitoring carried out on the Network, as described in clause 12.

2 Definitions

"the Company", "we"	The business named on the front page of this policy.
"the IT Provider"	The organisation named on the front page as IT provider, which manages the Network and Company Systems on the Company's behalf. <i>(If you manage your own IT, delete this definition and every reference to the IT Provider.)</i>
"the Network"	All wired and wireless networks operated by or for the Company, including any staff, guest and device Wi-Fi networks and any remote access to them.
"Company Systems"	Computers, devices, software, online services (including email and file storage) and accounts provided by the Company.
"Personal Device"	Any phone, tablet, laptop or other device not owned by the Company.

"User"	Any person who accesses the Network or Company Systems, including employees, temporary staff, contractors, visitors and guests.
"Credentials"	Any username, password, PIN or other means of signing in to the Network or Company Systems.

3 Scope

- 3.1 This policy applies to all Users and to every device that connects to the Network, whether owned by the Company or not, by cable or wirelessly, on site or remotely.
- 3.2 Visitors and guests using the guest Wi-Fi are bound by the parts of this policy that apply to them. **OPTIONAL**

4 Acceptance

- 4.1 Users who are given Credentials must confirm that they have read and accept this policy before or on receiving them, using the Company's online acknowledgement form or, where that is not practical, the paper acknowledgement on the final page.
- 4.2 A notice is displayed when signing in to Company computers. By signing in, the User confirms that their use is subject to this policy. **OPTIONAL**
- 4.3 Use of the Network or Company Systems constitutes acceptance of this policy as in force at the time of use.

5 Permitted use

- 5.1 The Network and Company Systems are provided for the Company's business purposes.
- 5.2 Reasonable personal use is permitted, provided that it does not interfere with the User's duties or the work of others, does not breach clause 6, and does not cause cost, risk or harm to the Company.
- 5.3 Reasonable access to social media is permitted on the same basis. The Company may limit or block access to social media for any User whose use it considers excessive.
- 5.4 Whether use is reasonable is for the Company to decide. Users who are unsure should ask their manager before proceeding.

6 Prohibited use

- 6.1 Users must not use the Network or Company Systems to:
- (a) commit or facilitate any unlawful act, or access, store or distribute unlawful material;
 - (b) access, store or distribute material that is obscene, pornographic, discriminatory, harassing, threatening or otherwise offensive;
 - (c) infringe copyright or other intellectual property rights, including by downloading or sharing pirated films, music or software;
 - (d) bypass, disable or interfere with any security, filtering or monitoring control, including by using a VPN, proxy, anonymiser, another person's Credentials, or a mobile hotspot on a Company computer;
 - (e) introduce malicious software, or knowingly follow malicious links;
 - (f) gain or attempt to gain unauthorised access to any system, account or data;
 - (g) cause damage to the Company, its customers or its reputation.

7 Filtering and blocking

- 7.1 The Company filters internet access on the Network. Categories blocked for all Users include: _____ *(for example malicious and fraudulent websites, adult and unlawful content, VPN and proxy services, online games).*
- 7.2 The Company may block further websites or services, for all Users or for an individual User or device, at its discretion.
- 7.3 A User who needs access to a blocked website for business purposes should request it under clause 14.

8 Credentials

- 8.1 Credentials are personal to the User. Users must not disclose their Credentials to anyone, including colleagues, or allow anyone else to use them. Activity carried out with a User's Credentials is attributed to that User.
- 8.2 Neither the Company nor the IT ProviderThe Company will never ask a User for their password.
- 8.3 Users must choose passwords in line with the Company's password guidance and must report immediately any suspicion that their Credentials are known to another person.

9 Company devices

- 9.1 Users must not install software, change security settings, or connect removable storage or other devices not supplied by the Company to Company computers, unless authorised.
- 9.2 Users must lock or sign out of Company computers when leaving them unattended, and take reasonable care of Company equipment.
- 9.3 Company devices may be managed using device management and security software, which records the information described in clause 12. Users must not remove, disable or interfere with that software.

- 9.4 The Company and the IT Provider may connect remotely to Company devices to support, maintain, update or secure them. Where practical, a notice is displayed on the device before a remote session begins. Where a device is unattended, or where immediate action is needed to protect the Network, Company Systems or Company information, a session may proceed without the User's agreement. **OPTIONAL**
- 9.5 Company devices and accounts are provided for the Company's purposes. Users should not store personal information on them, and the Company may access information stored on Company devices and accounts where necessary for legitimate business purposes, including security investigations, support and business continuity.

10 Email, data and information security

- 10.1 Company information must be stored in the Company's own systems and not on personal accounts or removable storage.
- 10.2 Users must not forward Company email to personal accounts, and must take care with unexpected emails, links and attachments, reporting any that appear suspicious.

11 Personal Devices **OPTIONAL**

- 11.1 Users may connect Personal Devices to the staff Wi-Fi using their own Credentials. Personal Devices receive internet access only and are not given access to Company Systems on the Network.
- 11.2 While connected to the Network, Personal Devices are subject to this policy, including filtering under clause 7 and monitoring under clause 12.
- 11.3 The Company does not manage Personal Devices and does not access their contents.

12 Monitoring

- 12.1 The Company monitors use of the Network for the purposes of security, the operation of the Network, and ensuring compliance with this policy.
- 12.2 The information recorded and the limits of monitoring are set out below. *(Change each row to match what your systems actually record.)*

Item	Detail
Information recorded	_____ <i>For example: the applications, services and categories of website used; the times and volume of use; the User and device concerned; sign-ins to Company Systems; and attempts to reach blocked or malicious websites.</i>
Company devices	_____ <i>For example: hardware and software inventory; update status; device health; security events; and the User signed in.</i>
Not recorded	The content of communications, or information entered or viewed on encrypted (https) websites. The contents of Personal Devices. Keystrokes, screen contents, webcam or microphone on any device, other than the screen during a remote support session under clause 9.4.
Access	_____ (for example the Company's management and whoever looks after its IT, as necessary to operate and protect the Network).
Reporting	Management receive summaries of Network use every _____. Management may request a report on a specific User or device where there is a legitimate concern.
Retention	Up to _____ days, after which it is deleted.

- 12.3 The Company will not carry out covert monitoring except in exceptional circumstances permitted by law.

13 Data protection

- 13.1 Monitoring information is personal data and is processed by the Company in accordance with UK data protection law. The IT Provider processes it on the Company's behalf.
- 13.2 Users may request access to personal data held about them, or raise a concern, by contacting _____. Users may also complain to the Information Commissioner's Office (ico.org.uk).

14 Reporting and requests

- 14.1 Users must report without delay, to _____: any suspected security incident (including clicking a suspicious link or disclosing Credentials); and the loss or theft of any Company device, or of a Personal Device holding Company information.
- 14.2 Requests to unblock a website or install software should be made to _____.

15 Breach of this policy

- 15.1 Where the Company considers that this policy has been breached, it may, according to the seriousness of the breach:
- (a) block specific websites or services for the User or device concerned;
 - (b) suspend or withdraw the User's or device's access to the Network;
 - (c) suspend or withdraw the User's use of Company computers or other devices.
- 15.2 The Company may take any of these steps immediately where it considers it necessary to protect the Network, Company Systems or Company information.

16 Leaving the Company

- 16.1 A User's access ends when their work with the Company ends. Users must return all Company equipment and remove the staff Wi-Fi and any Company accounts from their Personal Devices.

17 Ownership, review and approval

- 17.1 This policy is owned by _____ (*name and role*) on behalf of the Company and will be reviewed at least annually, or sooner if the Company's systems change. Users will be notified of any changes.
- 17.2 This policy is based on a template published by Cryptal Media Group Ltd. for general information. Cryptal Media Group Ltd. does not give legal, HR or employment advice, and neither the template nor this policy constitutes legal advice. The Company has reviewed and approved this policy and is responsible for its content and application. The Company may wish to obtain its own legal or HR advice, including on how this policy relates to contracts of employment.

APPROVAL

Approved for the Company by	Position	Signature	Date

ACKNOWLEDGEMENT

Confirming you have **read this policy**

Online (preferred). Complete the acceptable use policy acknowledgement form at:

_____. *(Delete this paragraph if you only use paper.)*

On paper. By signing below, I confirm that I have read and understood the Acceptable Use Policy of _____ at the version shown, that I agree to comply with it, and that I understand my use of the Network and Company Systems is monitored as described in clause 12.

Name	Signature	Date	Policy version

Keep signed paper acknowledgements with your staff records. A new acknowledgement is needed whenever the policy version changes.