Halo Benefits

POLICY

Acceptable Use Policy

Sets out how our people use devices, accounts, email and AI tools safely and responsibly.

UPDATED	VERSION	NEXT REVIEW
23 November 2026	2.0	November 2027

Halo Benefits Ltd · Owner: Alexander Dick, Head of Security & Operations · Classification: Internal & Public

Document control

Policy owner	Alexander Dick, Head of Security & Operations
Approved by	Board of Directors
Date approved	23rd November 2026
Next Review Date	23th November 2027
Review frequency	Annually
Applies to	All directors, employees and contractors, and every device or account used for Halo Benefits Ltd work
Related policies	Information Security Policy, Access Control Policy, Responsible AI Policy

Version history

Version	Date	Summary of changes	Author
1.0	30 Oct 2026	First issue	Alexander Dick
2.0	23 Nov 2026	Rebranded and restructured for clarity and readability	Dionne Clarke

Contents

1. Purpose of the policy ... 3
2. Scope ... 3
3. Device standards ... 3
4. Personal devices and removable media ... 4
5. Accounts and email ... 4
6. Using AI tools ... 4
7. Responsible use and working remotely ... 5
8. Monitoring and acknowledgement ... 5
9. Roles and responsibilities ... 5
10. Breaches and exceptions ... 6
11. Review ... 6

1. Purpose of the policy

This policy sets out what our people must and must not do when using devices, accounts, email, the internet and AI tools for Halo Benefits Ltd work.

We are a remote-first company and all of our systems are in the cloud, so the security of each person's device and accounts is a large part of how we keep your data safe.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and to all directors, employees and contractors. It covers every device or account used to access our information or systems, whether company-provided or personally owned.

3. Device standards

Any laptop, desktop, tablet or phone used to access Confidential or Restricted information must meet this baseline:

Requirement	What it means
Encryption	Full-disk encryption switched on
Screen lock	Locks after no more than 5 minutes, protected by a password, PIN or biometric
Updates	Operating system and browser updates installed within 14 days, and critical security updates as soon as practicable. Unsupported operating systems are not allowed.
Protection	Firewall and malware protection switched on
Standard accounts	Day-to-day work is done without administrator rights where possible
Software	Installed only from official sources and kept up to date
Registration	Recorded in our asset register

Compliance is confirmed by a signed device declaration at onboarding and every year, and is checked as part of our Cyber Essentials assessment.

4. Personal devices and removable media

- Personal devices that do not meet the baseline above and are not registered must never be used to access customer data, source code or live systems.
- A personal phone may be used for work email, chat and sign-in prompts only if it meets the baseline and is registered.
- Shared or public computers must never be used for work.
- USB drives, external disks and memory cards must not be used for customer data. Files are shared through approved cloud services instead.
- Customer personal data is only downloaded to a device when a task requires it, and is deleted as soon as the task is complete. Live customer data is never copied into development or test systems.

5. Accounts and email

- Everyone uses their own account only, and never shares passwords or sign-in devices.
- A password manager and multi-factor authentication must be used, as set out in our Access Control Policy.
- Passwords and other secrets are never pasted into email, chat, documents or AI tools.
- Work is done in company accounts, not personal email, and work email is never automatically forwarded to personal accounts.
- Unexpected attachments or links, changes to payment details and urgent requests for money or passwords are treated as possible phishing. They are checked through a separate channel before anyone acts, and reported.
- Restricted information is shared through secure links to named people rather than as email attachments wherever possible.

6. Using AI tools

- Only AI tools approved under our Responsible AI Policy may be used with company information.
- Customer personal data (including pay, dependant and health information) and other Restricted information must never be entered into an AI tool that is not approved for that data.

- AI coding assistants may help with source code, but are never given access to live systems or customer data. Code they produce goes through the same review and testing as code written by our team.
- People remain responsible for any AI output they use, and anything AI-generated that reaches a customer is reviewed by a person first.

7. Responsible use and working remotely

- Company systems must never be used for anything illegal, harassing or discriminatory, or that could damage our reputation.
- Security controls must never be bypassed or switched off.
- Browser extensions that can read web pages are only allowed if they are from a reputable publisher and genuinely needed.
- Screens are locked whenever someone steps away, and customer information is never discussed where it could be overheard.
- Trusted networks are used wherever possible. On public Wi-Fi, only secure (encrypted) services are used and Restricted data is avoided.
- Limited personal use of company devices is acceptable if it does not affect security or work.
- Lost or stolen devices are reported immediately, so that access can be removed and the device wiped.

8. Monitoring and acknowledgement

We may review logs from our own systems to protect security and investigate incidents. Any monitoring is proportionate and in line with data protection law, and our people are told about it through this policy.

Every new starter reads and signs this policy before getting access to our systems, and confirms it again each year as part of security awareness training.

9. Roles and responsibilities

- **Everyone:** follows this policy and keeps their devices compliant.
- **Line managers:** make sure their team has signed this policy and completed the device declaration.

- **Head of Security & Operations:** maintains the asset register and the list of approved tools, checks compliance and handles reports of loss, theft or misuse.

10. Breaches and exceptions

Signed acknowledgements and device declarations are kept with training records. Misuse may lead to disciplinary action, removal of access or termination of contract.

Any exception (for example, a device that temporarily cannot be updated) must be approved in advance by the Head of Security & Operations, be time-limited and be recorded.

11. Review

This policy is reviewed annually, and sooner after any significant change, including changes to the device standards required for Cyber Essentials. The Head of Security & Operations proposes changes and the Board of Directors approves them.

> QUESTIONS ABOUT THIS POLICY?
> Contact Alexander Dick, Head of Security & Operations, at security@halobenefits.co.uk.