COMPANY POLICY · UNITED KINGDOM

EXTERNAL COMMUNICATION & VENDOR VERIFICATION POLICY

Standards for email, telephone, messaging, cold outreach and supplier verification under UK law

COMPANY	ADD BOOST 360 Limited, registered in England and Wales, company number 16095942, registered office 124 City Road, London, EC1V 2NX
POLICY OWNER	Director, ADD BOOST 360 Limited
APPROVED BY	Board of Directors
VERSION	1.0
EFFECTIVE DATE	November 2026
NEXT REVIEW	November 2027, or sooner if the law or a serious incident requires it
APPLIES TO	Directors, employees, staff panel users, contractors, agents and anyone acting for the company
CONTACT	info@addboost360.com · +44 7441 396776

Policy statement

> No business inquiry, meeting request, partnership or supplier relationship goes further until the sender is verified under this policy. It applies to every channel and every person who speaks for ADD BOOST 360 Limited.

CONTENTS

1. Purpose and scope
2. UK legal and regulatory framework
3. Definitions
4. Roles and responsibilities
5. Mandatory sender identification
6. Verification procedure
7. Email
8. Telephone, SMS, WhatsApp and video calls
9. Website forms, social media, post and visits
10. Outbound marketing and cold outreach (PECR)
11. Vendor, supplier and partner due diligence
12. Payment and bank-detail change controls
13. Unverified, suspicious and phishing contact
14. Exceptions
15. Data protection, recording and retention
16. Training, monitoring, breaches and review
17. Changes to this policy

Appendix A: Standard response templates

Appendix B: Verification checklist and log

Sources

1. PURPOSE AND SCOPE

This policy sets the minimum checks staff must complete before engaging with any external business contact. Its aims are to:

- protect company, customer and staff data from phishing, impersonation and social engineering
- stop invoice, payment and bank-detail fraud
- keep our marketing and calls within UK law
- make every external contact traceable to a named, accountable person and organisation

Channels covered: email, telephone and voicemail, SMS, WhatsApp and other messaging apps, video calls, the website contact and enquiry forms, social media (including LinkedIn messages), post and in-person visits.

Contacts covered: B2B inquiries, cold outreach, partnership proposals, suppliers, vendors, contractors, agencies, recruiters and anyone asking for company information.

Not restricted by this policy: genuine customers and members of the public using our services, job applicants, people exercising data protection rights, and regulators or law enforcement. Section 14 sets out how these are handled.

2. UK LEGAL AND REGULATORY FRAMEWORK

This policy is written to meet the UK laws below. Where this policy and the law differ, the law wins.

Law or rule	What it means for us
UK GDPR and Data Protection Act 2018	Personal data collected while verifying contacts must be lawful, minimal, secure and kept no longer than needed
Data (Use and Access) Act 2025	Amends UK GDPR and PECR; its data protection and PECR provisions are now in force. PECR fines rise to £17.5 million or 4% of worldwide turnover
Privacy and Electronic Communications Regulations 2003 (PECR)	Rules for marketing emails, texts and calls, including TPS and CTPS screening
Company, LLP and Business (Names and Trading Disclosures) Regulations 2015	Our business emails, letters and website must show our registered name, number, place of registration and registered office
Economic Crime and Corporate Transparency Act 2023	Created the failure to prevent fraud offence (in force 1 September 2025). It targets large organisations, but its six principles are good practice and large clients may require them of us
Companies House identity verification	Mandatory since 18 November 2025 for directors and PSCs; lets us check a UK company's officers are verified
Fraud Act 2006 and Computer Misuse Act 1990	Impersonation, phishing and unauthorised access are crimes we report
Bribery Act 2010	No gifts, hospitality or payments to win or keep business
Investigatory Powers Act 2016 and the 2018 Interception by Businesses Regulations	Govern any recording or monitoring of calls and messages
Equality Act 2010	Verification must be applied the same way to everyone and must not discriminate

3. DEFINITIONS

Term	Meaning
External party	Any person or organisation that is not a director, employee or authorised contractor of ADD BOOST 360 Limited
B2B inquiry	Any business proposal, sales pitch, partnership offer, supplier approach or request for a meeting

Term	Meaning
Verified contact	An external party who has passed the checks in sections 5 and 6, recorded in the verification log
Corporate email	An address on the organisation's own domain, matching its website, such as name@company.co.uk
Free webmail	Consumer email services such as gmail.com, outlook.com, hotmail.com, yahoo.com, icloud.com and proton.me
Independent channel	A phone number, email or address that staff find themselves from an official source, never one supplied in the message being checked
Verification Lead	The director, or a person the director names in writing, who approves verifications and handles escalations
Corporate subscriber	Under PECR, a company, LLP, Scottish partnership or government body. Sole traders and other partnerships are individual subscribers

4. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Board of Directors	Approves this policy, sets risk appetite, receives incident reports
Director (policy owner)	Keeps the policy current, approves high-risk vendors and any exception, signs off bank-detail changes
Verification Lead	Runs checks, keeps the verification log, decides on escalations, reports incidents
Data protection lead	Advises on lawful handling of personal data, retention, data subject requests and breach reporting to the ICO within 72 hours where required
All staff and staff-panel users	Follow sections 5 to 13, use only company channels, report anything suspicious at once
Contractors and agents	Follow this policy when acting for the company; contracts must require it

5. MANDATORY SENDER IDENTIFICATION

ADD BOOST 360 Limited does not engage with anonymous, unverified or generic B2B inquiries. Before staff share internal contact details, book a meeting or discuss business needs, the external party must provide all of the following.

#	Required detail	How staff check it
1	Full legal name of the person making contact	Matches their email signature, LinkedIn profile and company website team page where one exists
2	Official corporate email on the organisation's registered domain	Domain matches the company website; free webmail is refused for B2B outreach

#	Required detail	How staff check it
3	Job title and the organisation's registered company name	Name matches the official register (Companies House for UK companies, or the equivalent overseas register)
4	Country of operation and registered business address	Address matches the register; a virtual office alone is treated as higher risk
5	Company registration number (or overseas equivalent) and VAT number where registered	Number is active on the register; UK VAT numbers checked with HMRC's online VAT check
6	Verifiable digital presence: official website and an active LinkedIn profile for the person or company	Website is live, shows trading disclosures and is not newly registered; profile is established, not newly created

Free webmail. Inquiries sent from free webmail addresses such as @gmail.com, @outlook.com, @hotmail.com or @yahoo.com are not accepted for B2B outreach. The sender is asked to write again from their corporate address. This rule does not apply to the groups in section 14, such as customers, sole traders using our services, job applicants and people making data protection requests.

Sole traders and small firms. A genuine sole trader may have no company number or corporate domain. They may be verified instead with a trading website, an established business profile, a business bank account in the same trading name and a call-back on an independently found number. The Verification Lead must approve this route.

6. VERIFICATION PROCEDURE

Checks scale with risk: the more access, money or data involved, the more evidence is needed and the more senior the sign-off.

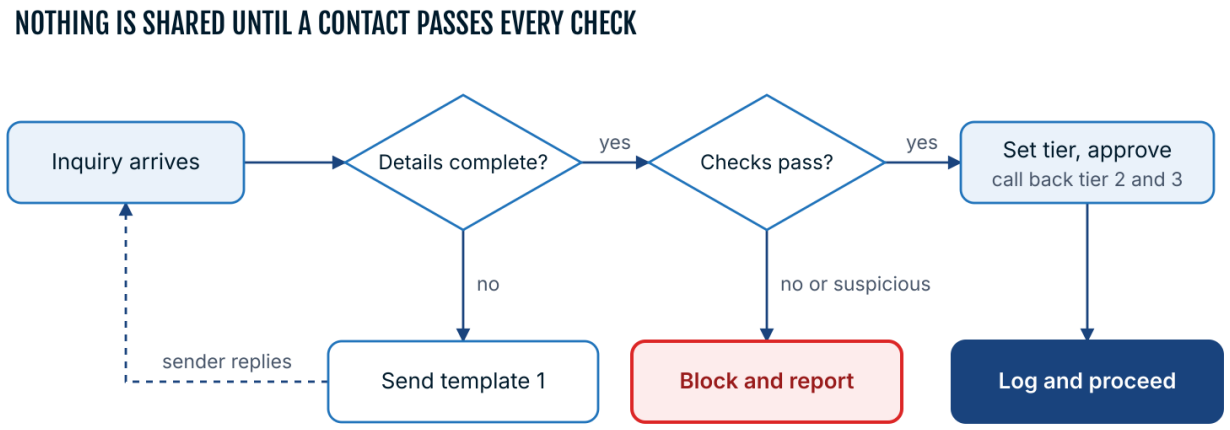
Tier	Typical contact	Minimum checks	Approved by
1 – Low	General B2B inquiry, request for public information, event invitation	Section 5 items 1, 2 and 6	Any trained staff member
2 – Medium	Meeting request, partnership proposal, sharing non-public business information	All of section 5, plus a register check	Verification Lead
3 – High	New supplier or vendor, anyone to be paid, anyone given system or data access, any contract	All of section 5, section 11 due diligence, plus a call-back on an independently found number	Director

Steps for every new contact

1. Do not reply with any internal details. Use the standard verification request (Appendix A, template 1) if details are missing.
2. Check the sender's domain against their official website. Look for look-alike spelling, extra words or a different country ending.

3. Look the organisation up on the official register. For UK companies, confirm it is active and its officers are identity-verified.
4. Find the organisation's phone number yourself from the register or its official website. Never use the number in the message.
5. For tier 2 and 3, call that number and confirm the person works there and sent the request.
6. Record the result in the verification log (Appendix B) before going further.
7. If any check fails or feels wrong, stop and follow section 13.

Verification lasts 12 months for tier 1 and 2 contacts. Tier 3 suppliers are re-checked every year and whenever their ownership, bank details or contact people change.



A contact who fails a check is blocked and reported; one with missing details is asked once and checked again when they reply.

7. EMAIL

Inbound email

- Check the real sender address, not just the display name. Treat reply-to addresses that differ from the sender as suspicious.
- Do not open attachments or click links from unverified senders. Open shared files only after the sender is verified.
- Never enter passwords, one-time codes or payment details from a link in an email. Go to the site directly.
- Watch for urgency, secrecy, unusual payment requests, changed bank details and messages that claim to be from a director.

Outbound email

- Use only company email addresses on the addboost360.com domain. Personal email accounts must never be used for company business.
- Every business email must carry the company signature with these trading disclosures:

> [Name] | [Job title]
> ADD BOOST 360 Limited

Registered in England and Wales | Company No. 16095942
Registered office: 124 City Road, London, EC1V 2NX
www.addboost360.com

- Send personal or confidential data only to verified recipients. Use encrypted links or password-protected files, and send the password by a different channel.
- Use BCC for group emails to external people so addresses are not exposed.

Email security

- Keep SPF, DKIM and DMARC records in place for addboost360.com so others cannot easily fake our address.
- Turn on two-factor sign-in for every company mailbox.
- Report any account that may be compromised to the Verification Lead at once.

8. TELEPHONE, SMS, WHATSAPP AND VIDEO CALLS

Incoming calls

- Caller ID can be faked. A caller's claim to be a bank, client, supplier, HMRC, police or a director proves nothing.
- Take the caller's name, organisation and reason, then end the call. Ring back on a number you found yourself from an official source.
- Never give out staff names, direct numbers, mobile numbers, schedules, system details or customer information to an unverified caller.
- Never read out or confirm one-time codes, passwords or payment details over the phone. No genuine organisation needs them.

Voicemail, SMS and messaging apps

- Treat unexpected texts and WhatsApp messages as unverified, even if the name shown is familiar.
- A new number claiming to be a known contact ("I've changed my phone") must be confirmed by calling the old, known number.
- Company business on WhatsApp or other apps is allowed only with verified contacts, on company-approved accounts, with two-step verification turned on.
- Do not share staff WhatsApp or personal mobile numbers with unverified senders.

Video calls

- Join only links sent from a verified contact's corporate email.
- Be aware that voice and video can be faked. Any request for payment, data or access made on a call must be confirmed again through section 12.

Call recording

- Calls are recorded only if the company decides to and records why. Callers and staff must be told at the start of the call, and recordings are kept under section 15.

9. WEBSITE FORMS, SOCIAL MEDIA, POST AND VISITS

- **Website enquiry forms:** customer enquiries are answered normally. B2B pitches sent through the form are verified under section 5 before any reply beyond template 1.
- **Social media and LinkedIn:** connection requests and direct messages are not proof of identity. Move business talks to verified corporate email before sharing anything. Only authorised staff may speak for the company on social media.
- **Post:** check letters that ask for payment or changes against the sender's details on the official register. Treat unexpected invoices as suspicious until matched to a purchase order.
- **Visitors:** visitors must be expected, give their name and organisation, be signed in and be accompanied. Do not let anyone follow you through a secured door.
- **Requests for staff or customer lists:** refuse them. They are a common first step in fraud.

10. OUTBOUND MARKETING AND COLD OUTREACH (PECR)

Our own outreach must meet the standard we ask of others. Breaches of PECR's marketing rules can now cost up to £17.5 million or 4% of worldwide turnover.

Channel	To companies and LLPs (corporate subscribers)	To sole traders, some partnerships and individuals
Marketing email or SMS	Allowed without prior consent; always identify ourselves and offer a simple opt-out	Only with consent, or the soft opt-in for existing customers
Live marketing call	Only after screening against the CTPS and our own do-not-call list	Only after screening against the TPS and our own do-not-call list
Automated recorded call	Only with prior specific consent	Only with prior specific consent

- Always state the company name, never hide or fake the number we call from, and give a working way to opt out.
- Act on every opt-out at once and record it on the suppression list. Never contact that person or business again for marketing.
- UK GDPR still applies to named business contacts, such as firstname@company.com. Tell them where we got their details and how to object.
- Do not buy or rent contact lists unless the seller proves the data was collected lawfully and screened against TPS and CTPS.

11. VENDOR, SUPPLIER AND PARTNER DUE DILIGENCE

No supplier is paid, given system access or handed personal data until the checks below are complete and the director has signed off.

- ☐ Company is active on the official register; name, number and registered address match the invoice and contract
- ☐ Directors and people with significant control are listed; for UK companies, identity verification status checked
- ☐ Not on the UK sanctions list (OFSI consolidated list)
- ☐ Website, trading history and reviews look genuine; domain not newly registered
- ☐ VAT number checked where one is charged
- ☐ Bank account name matches the company name; confirmed by a call-back to an independently found number
- ☐ Written contract in place; if they handle personal data, a data processing agreement under UK GDPR Article 28
- ☐ Security basics confirmed for anyone with system or data access (two-factor sign-in, data stored securely, breach notice duty)
- ☐ International transfer safeguards in place if they process personal data outside the UK
- ☐ Anti-bribery and conflict-of-interest confirmation obtained

Each completed checklist is saved with the verification log. Repeat it every year and when ownership, bank details or key contacts change.

12. PAYMENT AND BANK-DETAIL CHANGE CONTROLS

Any request to pay, or to change where we pay, is treated as possible fraud until confirmed by phone on a known number.

1. Never change bank details because of an email, letter, text or call alone, even from a known contact's address.
2. Call the supplier on the number already held on file or found on the official register. Never use contact details in the request.
3. Confirm the old and new account details and the reason for the change with a named person.
4. A second person checks the change before it is saved. The director approves it.
5. Send a small test payment for new or changed details, then confirm receipt by phone before paying the full amount.
6. Urgent or secret payment requests, including ones that appear to come from a director, are always checked by a call to that director's known number.

If money has been sent to a fraudster, contact our bank immediately, then report to Report Fraud (section 13).

13. UNVERIFIED, SUSPICIOUS AND PHISHING CONTACT

Unverified (details missing but not suspicious)

- Share nothing: no direct phone numbers, WhatsApp contacts, staff names or project details.
- Send the standard verification request (Appendix A, template 1) once. If there is no reply in 14 days, close it.

Suspicious or automated

- Do not reply, click, open attachments or call numbers in the message.
- Mark it as spam or phishing in the mail system and block the sender.
- Tell the Verification Lead the same day, with a screenshot or the forwarded message.

Where to report

What	Report to
Phishing email	Forward to report@phishing.gov.uk (National Cyber Security Centre)
Scam text message	Forward to 7726 (free)
Fraud or cyber crime, including money lost	Report Fraud: reportfraud.police.uk or 0300 123 2040 (replaced Action Fraud on 4 December 2025)
Money sent in error or to a fraudster	Our bank, at once
Personal data exposed	Data protection lead; the ICO within 72 hours if the breach is likely to risk people's rights
Unlawful marketing calls or messages received	The ICO

Staff who report a mistake quickly, such as clicking a link, will not be punished for reporting it. Fast reporting limits the damage.

14. EXCEPTIONS

The B2B rules in section 5, including the free-webmail rule, must not be used to turn away people who have a right or a good reason to contact us.

Who	How we handle them
Customers and members of the public	Served normally from any email address. Account changes are confirmed through their signed-in account or a known contact detail
Job applicants	Accepted from any email address; handled under our recruitment privacy notice
Data protection requests (access, deletion, objection)	Accepted by any channel and any email address. Ask only for the identity proof reasonably needed; the one-month time limit starts once identity is confirmed

Who	How we handle them
Complaints	Accepted from anyone and logged
Regulators, courts and law enforcement	Verified by calling the body on its published number, then passed to the director
Emergencies	Safety comes first; record and verify afterwards
Any other exception	Only the director may approve it, in writing, with the reason logged

15. DATA PROTECTION, RECORDING AND RETENTION

We collect only the details needed to verify a contact, under our legitimate interest in preventing fraud and protecting our systems. Our privacy notice tells external contacts this.

Record	Kept for	Then
Verification log entry for a contact we did not work with	12 months	Deleted
Verification and due diligence for suppliers we worked with	6 years after the relationship ends	Deleted
Spam and phishing reports	12 months	Deleted
Marketing suppression (opt-out) list	For as long as we do marketing	Kept so we never contact them again
Call recordings (if used)	90 days, unless needed for a complaint or dispute	Deleted
Incident and fraud reports	6 years	Deleted

- Store records only in company systems, with access limited to those who need it.
- Do not copy identity documents unless they are truly needed. Delete copies once checks are done.
- Requests from people for their verification data are handled under section 14.

16. TRAINING, MONITORING, BREACHES AND REVIEW

- **Training:** all staff and staff-panel users complete training on this policy when they join and every year after. Training covers phishing, phone scams, fake invoices, deepfake calls and reporting.
- **Monitoring:** the Verification Lead reviews the verification log every quarter. Company systems may be monitored for security, as set out in the staff privacy notice.
- **Breaches of this policy:** a breach may lead to disciplinary action, up to dismissal. For contractors it may end the contract. A breach that was reported honestly and promptly will be treated as a learning point.

- **Review:** the policy is reviewed every year, after any serious incident and when the law changes.
- **Acknowledgement:** each staff member signs to confirm they have read and will follow this policy.

17. CHANGES TO THIS POLICY

ADD BOOST 360 Limited may change this policy at any time, based on the circumstances. Typical reasons are:

- changes in UK law, regulation or official guidance
- new fraud, phishing or security threats
- changes to our services, systems or ways of working
- lessons learned from an incident or review

The version number and date on the cover show the current edition, and the latest version published on our website applies from the date it is published. Significant changes are summarised when the new version is published. Where a change directly affects a supplier or partner we work with, we will tell them.

APPENDIX A: STANDARD RESPONSE TEMPLATES

Template 1 – Verification request (email)

> Subject: Verification required before we can respond
>
> Thank you for contacting ADD BOOST 360 Limited.
>
> To protect our clients and our business, we only engage with verified organisations. Please reply from your official company email address with:
>
> - your full name and job title
> - your organisation's registered name, registration number and country
> - your registered business address
> - your company website and LinkedIn profile
>
> We do not respond to business proposals sent from personal or free email accounts. Once we have verified your details, a member of our team will be in touch.
>
> Kind regards,
> [Name] | ADD BOOST 360 Limited
> Registered in England and Wales | Company No. 16095942 | Registered office: 124 City Road, London, EC1V 2NX

Template 2 – Telephone script for unverified callers

> "Thank you for calling ADD BOOST 360. For security, we don't discuss business details or share contact information on an unscheduled call. Could I take your full name, your organisation and the reason for your call? Please also send your request from your company email to info@addboost360.com. Once we've verified your details, we'll call you back on your organisation's official number."

Template 3 – Declining after failed verification

> Subject: Your inquiry to ADD BOOST 360 Limited
>
> Thank you for your message. We have not been able to verify the details provided, so we are unable to take this inquiry further. If you believe this is an error, please write to info@addboost360.com from your official company email with your organisation's registration details.
>
> ADD BOOST 360 Limited

Template 4 – Marketing opt-out confirmation

> You have been removed from ADD BOOST 360 Limited marketing. We will not contact you for marketing again. We keep your details only on our suppression list so this request is respected.

APPENDIX B: VERIFICATION CHECKLIST AND LOG

Quick checklist (tick before replying with any internal detail)

- ☐ Full legal name given
- ☐ Corporate email on the company's own domain (not free webmail)
- ☐ Job title and registered company name given
- ☐ Company is active on the official register; number and address match
- ☐ Website and LinkedIn presence look genuine
- ☐ Phone number found independently and call-back made (tier 2 and 3)
- ☐ Risk tier set and approval obtained
- ☐ Entry added to the log below

Verification log

Date	Contact name	Organisation	Co. no.	Channel	Tier	Checks passed	Outcome	Checked by	Approved by

Staff acknowledgement

I have read the External Communication & Vendor Verification Policy of ADD BOOST 360 Limited and agree to follow it.

Name	Role	Signature	Date

SOURCES

- ICO: Business-to-business marketing
- ICO: Telephone marketing
- ICO: Direct marketing and data protection
- GOV.UK: Data (Use and Access) Act factsheet, PEC Regulations
- GOV.UK: Failure to prevent fraud offence
- GOV.UK: Companies House identity verification
- legislation.gov.uk: Trading Disclosures Regulations 2015, reg. 25
- legislation.gov.uk: Interception by Businesses Regulations 2018
- GOV.UK: Report phishing
- Report Fraud service

This policy is a practical guide, not legal advice. Have a UK solicitor review it before adoption.