BOOST TA LTD Data Protection & Cyber Security Policy

Document Reference: BOOST-GOV-POL-001
Document Owner: Directors
Approved By: Giles Donovan & William Roberts
Issue Date: 04 September 2026
Review Date: 03 September 2027

1. Policy Statement and Purpose

BOOST TA Ltd is committed to protecting personal information, confidential business information and Company systems from unauthorised access, loss, misuse, alteration, disclosure or destruction.

The Company will process personal information lawfully and responsibly and maintain proportionate technical and organisational security measures appropriate to the information, systems and risks involved.

BOOST will:

- Comply with applicable UK data protection legislation.
- Collect and use personal information only where there is a lawful and legitimate purpose.
- Be clear about how and why personal information is used.
- Limit personal information to what is necessary for the intended purpose.
- Take reasonable steps to keep information accurate and up to date.
- Retain information only for as long as required.
- Protect personal and confidential information against unauthorised or unlawful processing, accidental loss, destruction or damage.
- Respect the rights of individuals in relation to their personal information.
- Control access to information according to business need.
- Use appropriate security controls for Company devices, systems, accounts and data.
- Maintain suitable arrangements for backups, software updates, malware protection and access security.
- Promote secure password and multi-factor authentication practices.
- Provide appropriate data protection and cyber security information, instruction or training to personnel.

- Require suspected data breaches, cyber incidents, phishing attempts and loss of Company information or devices to be reported promptly.
- Assess and respond to personal-data breaches in accordance with applicable reporting requirements.
- Review data protection and cyber security arrangements periodically and following significant incidents or changes.

This Policy applies alongside any supporting privacy notices, records, contracts, procedures and information-security arrangements maintained by BOOST TA Ltd.

2. Scope

This Policy applies to all personal information, confidential information and Company data processed, stored, accessed or transmitted by BOOST TA Ltd.

It applies to:

- Directors.
- Employees.
- Temporary workers.
- Contractors and subcontractors.
- Consultants.
- Agency personnel.
- Other persons who are authorised to access BOOST information or systems.

2.1 Information Covered

This Policy applies to information including:

- Employee and worker information.
- Applicant and recruitment information.
- Client and customer information.
- Supplier and subcontractor information.
- Contact details.
- Identification information.
- Financial and payment information.
- Training and competence records.

- Health and safety records containing personal information.
- Accident, incident and investigation records.
- Photographs or video containing identifiable individuals.
- CCTV information, where applicable.
- Emails and correspondence.
- Commercially sensitive information.
- Contracts, quotations and project information.
- Drawings, specifications and technical documents.
- Usernames, account details and system information.
- Any other personal, confidential or commercially sensitive information held by BOOST.

Additional safeguards will be applied where information is particularly sensitive or where the potential consequences of loss, disclosure or misuse are greater.

2.2 Systems and Locations

The Policy applies to information held or accessed through:

- Company computers and laptops.
- Mobile phones and tablets.
- Company email accounts.
- Cloud-based systems.
- Shared drives and document-management systems.
- MITTI and other approved business applications.
- Client or contractor systems accessed by BOOST personnel.
- Portable storage devices where specifically authorised.
- Paper records.
- Site documentation.
- Remote and home-working arrangements.
- Other approved systems used for Company business.

2.3 Personal and Company Devices

Company information will normally be accessed using approved Company devices, accounts and systems.

Where the use of a personal device is permitted for Company business:

- Access must be authorised where required.
- Appropriate device security must be enabled.
- Company information must not be unnecessarily downloaded or retained.
- Personal information must not be shared with unauthorised persons.
- Company accounts must not be shared.
- Lost, stolen or compromised devices must be reported promptly.
- BOOST may restrict or withdraw access where security requirements are not met.

2.4 Third Parties

Where BOOST shares information with or provides system access to a supplier, contractor, consultant or other third party, appropriate controls will be applied according to the nature of the information and risk involved.

This may include:

- Confidentiality requirements.
- Contractual data protection clauses.
- Restricted system access.
- User permissions.
- Secure methods of information transfer.
- Due diligence on service providers.
- Data processing agreements where required.
- Removal of access when it is no longer required.

Third parties must only use BOOST information for the authorised purpose and in accordance with applicable legal, contractual and security requirements.

2.5 Responsibility for Compliance

Everyone covered by this Policy is responsible for protecting the information and systems they use.

Personnel must:

- Follow this Policy and associated procedures.
- Use information only for legitimate business purposes.
- Protect passwords and account credentials.
- Prevent unauthorised access.
- Store information appropriately.
- Report suspected breaches, cyber incidents or loss of information promptly.
- Seek advice where they are uncertain about the correct handling of information.

Failure to follow this Policy may result in investigation and appropriate action in accordance with Company arrangements.

3. Data Protection Principles and Lawful Processing

BOOST TA Ltd will process personal information in accordance with the principles of UK data protection law.

Personal information will be:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Limited to information that is adequate, relevant and necessary.
- Kept accurate and, where necessary, up to date.
- Retained only for as long as required.
- Protected through appropriate technical and organisational security measures.
- Managed in a way that allows BOOST to demonstrate compliance with its data protection obligations.

3.1 Lawful Basis

Before processing personal information, BOOST will identify an appropriate lawful basis.

Depending on the activity, this may include:

- Consent.
- Performance of a contract.
- Compliance with a legal obligation.
- Protection of vital interests.
- Performance of a task in the public interest, where applicable.

- Legitimate interests pursued by BOOST or another party, where those interests are not overridden by the rights and interests of the individual.

Consent will not be relied upon where another lawful basis is more appropriate.

Where consent is used, it must be:

- Freely given.
- Specific.
- Informed.
- Unambiguous.
- Capable of being withdrawn.

3.2 Special Category Information

BOOST may occasionally process more sensitive personal information where required for legitimate business or legal purposes.

This may include information relating to:

- Health.
- Disability.
- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Trade union membership.
- Biometric information used for identification.
- Other information defined as special category data under applicable legislation.

Where special category information is processed, BOOST will ensure that:

- A lawful basis for processing applies.
- An additional condition for processing special category data applies.
- Access is restricted to those who genuinely require it.
- Appropriate security and confidentiality controls are maintained.
- The information is not collected or retained unnecessarily.

3.3 Criminal Offence Information

Criminal offence information will only be processed where BOOST has an appropriate lawful basis and legal authority to do so.

Access to such information will be restricted and appropriate safeguards will be applied.

3.4 Transparency and Privacy Information

Individuals will be provided with appropriate information about how their personal information is used.

Privacy information may include:

- The identity of BOOST TA Ltd.
- Contact details for data protection enquiries.
- The purposes for which information is processed.
- The lawful basis relied upon.
- Categories of information processed.
- Who information may be shared with.
- Relevant retention periods.
- Individual data protection rights.
- Information regarding international transfers where applicable.
- The right to raise concerns with the Information Commissioner's Office.

Privacy information will be kept under review and updated where processing activities materially change.

3.5 Data Minimisation

BOOST will only collect and retain personal information that is reasonably necessary for the relevant purpose.

Personnel should avoid:

- Collecting information simply because it may be useful later.
- Recording unnecessary personal opinions.
- Retaining duplicate records without justification.
- Sharing more information than is necessary.
- Including sensitive personal information in emails or documents where it is not required.

3.6 Accuracy

Reasonable steps will be taken to ensure that personal information is accurate and current.

Where inaccurate information is identified:

- It will be corrected where appropriate.
- Relevant records will be updated.
- Recipients of materially inaccurate information may be informed where required.
- Disputed information will be reviewed before further reliance is placed upon it.

3.7 Retention

Personal information will not be retained indefinitely without a valid reason.

Retention periods will take account of:

- Legal requirements.
- Contractual requirements.
- Employment requirements.
- Health and safety record requirements.
- Insurance requirements.
- Limitation periods.
- Client requirements.
- Legitimate business needs.

Information that is no longer required will be securely deleted, destroyed or anonymised as appropriate.

4. Roles and Responsibilities

BOOST TA Ltd will assign clear responsibility for data protection and cyber security so that personal information, confidential information and Company systems are appropriately managed.

4.1 Directors

The Directors are responsible for:

- Approving this Policy.
- Providing suitable resources for data protection and cyber security.
- Ensuring appropriate technical and organisational controls are maintained.
- Supporting compliance with applicable data protection requirements.
- Reviewing significant data protection or cyber security incidents.

- Ensuring appropriate action is taken where material weaknesses are identified.

4.2 Data Protection Lead

BOOST will appoint a suitable person to act as the Data Protection Lead.

The Data Protection Lead will:

- Provide a point of contact for data protection matters.
- Support implementation of this Policy.
- Maintain oversight of personal data processing activities.
- Coordinate responses to data subject requests.
- Support assessment and management of personal data breaches.
- Maintain appropriate breach and request records.
- Support review of privacy information and retention arrangements.
- Provide advice on data sharing and data protection requirements.
- Escalate significant concerns to the Directors.
- Liaise with the Information Commissioner's Office where required.

The role of Data Protection Lead does not automatically constitute appointment as a statutory Data Protection Officer.

4.3 Managers

Managers are responsible for:

- Ensuring personnel understand relevant data protection and cyber security requirements.
- Limiting access to information according to role and business need.
- Reporting changes that may require access permissions to be amended.
- Supporting completion of required training.
- Reporting suspected data breaches or cyber incidents promptly.
- Ensuring records within their area of responsibility are appropriately stored and retained.
- Escalating concerns where information is being handled insecurely.

4.4 IT and System Administration

Where IT support or system administration is provided internally or by an external provider, responsibilities may include:

- Managing user accounts and permissions.
- Applying appropriate security settings.
- Maintaining software updates and security patches.
- Maintaining malware protection.
- Supporting multi-factor authentication.
- Maintaining backup arrangements.
- Supporting secure recovery following system failure or cyber incident.
- Removing or disabling access where no longer required.
- Supporting investigation of suspected cyber security incidents.

External IT providers will be subject to appropriate confidentiality, security and data protection requirements where they have access to BOOST systems or information.

4.5 Employees, Workers and Contractors

All personnel are responsible for:

- Following this Policy.
- Protecting information from unauthorised access or disclosure.
- Using approved Company systems and accounts.
- Keeping passwords and authentication information secure.
- Locking devices when unattended.
- Taking reasonable care when sending emails or sharing information.
- Checking recipients before transmitting confidential or personal information.
- Avoiding suspicious links, attachments or downloads.
- Reporting suspected phishing, malware or account compromise.
- Reporting lost or stolen devices promptly.
- Reporting accidental disclosure or loss of information promptly.
- Securely disposing of records when authorised to do so.
- Completing required data protection and cyber security training.

4.6 Access Management

Access to personal, confidential and commercially sensitive information will be based on business need.

BOOST will apply appropriate controls including:

- Individual user accounts.
- Role-based permissions where available.
- Restricted access to sensitive information.
- Removal or amendment of access when roles change.
- Prompt removal of access when employment or engagement ends.
- Periodic review of access where appropriate.
- Multi-factor authentication where available and proportionate.

Shared user accounts should be avoided where individual accounts are reasonably available.

4.7 Confidentiality

Personnel must not disclose personal, confidential or commercially sensitive information to unauthorised persons.

Confidentiality obligations continue after employment, engagement or contractual relationships with BOOST end where applicable.

5. Information Security and Cyber Security Controls

BOOST TA Ltd will maintain proportionate technical and organisational controls to protect Company information, personal data and business systems from unauthorised access, loss, misuse, alteration, disclosure or destruction.

5.1 Approved Systems and Devices

Company information should be accessed and stored using approved systems, applications and devices.

Personnel must:

- Use authorised Company accounts.
- Avoid transferring Company information to unapproved personal accounts.
- Avoid using unauthorised cloud storage or file-sharing services.
- Keep Company devices physically secure.
- Report lost, stolen or compromised devices promptly.

- Follow any Company requirements for remote or home working.

5.2 Passwords and Authentication

Passwords must be sufficiently strong and difficult to guess.

Personnel must:

- Use unique passwords for Company systems.
- Not share passwords with other persons.
- Not reuse Company passwords for personal services.
- Use multi-factor authentication where enabled or required.
- Use an approved password manager where provided.
- Change passwords where compromise is suspected or required by the system.
- Not record passwords in insecure locations.

Passwords do not need to be changed routinely solely because a fixed period has elapsed unless required by the relevant system or there is reason to believe the password may have been compromised.

5.3 Device Security

Company devices will, where appropriate, be protected through measures such as:

- Password, PIN or biometric access controls.
- Automatic screen locking.
- Device encryption.
- Supported operating systems.
- Security updates and patches.
- Malware protection.
- Firewall protection.
- Restricted administrator access.
- Remote management or remote-wipe capability where available and appropriate.

Users must not deliberately disable security controls without authorisation.

5.4 Software and Updates

Only approved or authorised software should be installed on Company devices.

Security updates and patches should be applied within an appropriate timeframe.

Personnel must not:

- Install unapproved software that may introduce security risk.
- Circumvent security settings.
- Use unsupported software where an approved alternative is available.
- Ignore security warnings without appropriate review.

5.5 Email and Electronic Communication

Personnel must take reasonable care when sending or receiving information electronically.

Before sending personal, confidential or commercially sensitive information, users should:

- Confirm the correct recipient.
- Check email addresses carefully.
- Limit information to what is necessary.
- Use secure sharing methods where appropriate.
- Consider password protection or encryption where the sensitivity or risk justifies it.
- Avoid sending sensitive information to personal email accounts.

Where an email is sent to multiple external recipients who should not see each other's contact details, BCC or another suitable method should be used where appropriate.

5.6 Phishing and Suspicious Communications

Personnel must remain alert to suspicious emails, messages, links, attachments and requests.

Warning signs may include:

- Unexpected requests for payment.
- Requests to change bank details.
- Urgent requests for passwords or login information.
- Unexpected attachments.
- Suspicious links.
- Unusual requests from known contacts.
- Requests to bypass normal approval processes.

Where there is doubt, the request should be independently verified before action is taken.

Suspected phishing or fraudulent communications must be reported promptly.

5.7 Financial and Payment Fraud

Changes to supplier, subcontractor or other payment details should not be accepted solely on the basis of an email request.

Where appropriate, BOOST will independently verify significant changes using trusted contact information already held by the Company.

5.8 Secure Storage and Sharing

Personal and confidential information will be stored in a manner appropriate to its sensitivity.

Controls may include:

- Restricted folders.
- Role-based permissions.
- Secure cloud storage.
- Encryption.
- Password-protected documents where appropriate.
- Controlled physical storage.
- Secure file-transfer methods.

Information should only be shared with persons who have a legitimate need to receive it.

5.9 Paper Records

Paper records containing personal or confidential information will be:

- Stored securely when not in use.
- Protected from unauthorised viewing.
- Not left unattended in public or uncontrolled areas.
- Transported securely where necessary.
- Destroyed securely when no longer required.

5.10 Removable Media

USB drives, external drives and other removable storage devices should only be used where there is a legitimate business need.

Where used for personal, confidential or commercially sensitive information:

- The device should be approved where required.

- Encryption should be used where appropriate.
- The device must be kept secure.
- Information should be removed when no longer required.
- Loss of the device must be reported promptly.

5.11 Backups and Recovery

BOOST will maintain suitable backup arrangements for important business information and systems where required.

Backup arrangements should consider:

- Frequency.
- Security.
- Access restrictions.
- Separation from primary systems.
- Recovery capability.
- Periodic verification or testing where appropriate.

5.12 Remote and Public Access

When working remotely or using networks outside BOOST premises, personnel must take appropriate care to protect Company information.

Users should:

- Avoid accessing sensitive information where others can view the screen.
- Use trusted networks where reasonably practicable.
- Avoid unsecured public Wi-Fi for sensitive activities unless suitable protection is available.
- Lock devices when unattended.
- Prevent family members or other unauthorised persons from accessing Company devices or information.
- Store paper records securely.

5.13 Secure Disposal

Information and equipment will be disposed of securely when no longer required.

This may include:

- Shredding confidential paper records.
- Secure deletion of electronic records.
- Secure wiping of storage devices.
- Removing Company information from devices before disposal or reuse.
- Using approved disposal providers where appropriate.

5.14 Use of Artificial Intelligence

BOOST TA Ltd may use approved artificial intelligence tools to support legitimate business activities where their use is appropriate, secure and consistent with client, contractual and data protection requirements.

Personnel must not upload or enter personal, confidential, commercially sensitive, security-sensitive or client-controlled information into an AI system unless the system and proposed use have been approved.

Where AI is used, BOOST will:

- Use approved AI tools and Company accounts.
- Consider the sensitivity and ownership of information before it is entered into an AI system.
- Comply with client restrictions relating to AI, confidentiality and information security.
- Avoid using client information to train or improve third-party AI models unless expressly authorised.
- Minimise personal and confidential information included in prompts.
- Anonymise or redact information where reasonably practicable.
- Apply additional controls to security-sensitive drawings, plans, photographs, site information and infrastructure information.
- Review AI-generated content before it is relied upon, issued or used to make decisions.
- Not treat AI-generated information as automatically accurate.
- Maintain appropriate human oversight.

- Complete a data protection or AI risk assessment where the proposed use presents elevated risk.
- Report suspected disclosure of restricted information to an AI service as a potential information-security incident.

5.15 Information Security Risk Management

BOOST will identify and assess information-security and cyber-security risks proportionate to the nature of its information, systems, processing activities and business operations.

Risk assessment may consider:

- Confidentiality, integrity and availability of information.
- Personal and special category data.
- Client-controlled and commercially sensitive information.
- Cyber threats and system vulnerabilities.
- User access and authentication.
- Third-party and supply-chain risks.
- Cloud and software services.
- Remote and mobile working.
- Loss, theft or compromise of devices.
- Backup and recovery arrangements.
- New systems and technologies.
- Artificial intelligence.
- Significant changes to processing or business activities.

Where additional treatment is required, appropriate technical, organisational or contractual controls will be identified and implemented.

Significant information-security risks and treatment actions will be reviewed periodically and following material changes, incidents or identified weaknesses.

6. Individual Rights and Subject Access Requests

BOOST TA Ltd will respect the rights of individuals in relation to their personal information and will respond to valid requests in accordance with applicable data protection legislation.

6.1 Individual Rights

Depending on the circumstances, individuals may have the right to:

- Be informed about how their personal information is used.
- Request access to personal information held about them.
- Request correction of inaccurate or incomplete information.
- Request deletion of personal information where applicable.
- Request restriction of processing in certain circumstances.
- Object to certain types of processing.
- Request transfer of information where the right to data portability applies.
- Withdraw consent where processing is based on consent.
- Raise concerns regarding certain automated decision-making or profiling.
- Complain to the Information Commissioner's Office.

These rights are not absolute and may be subject to legal exemptions or limitations.

6.2 Subject Access Requests

An individual may request confirmation of whether BOOST processes their personal information and request access to that information.

Requests may be made verbally or in writing and do not need to use the words "Subject Access Request" to be valid.

Any member of personnel receiving a request for access to personal information must forward it promptly to the Data Protection Lead.

6.3 Recording the Request

The Data Protection Lead will maintain a suitable record of each data protection request.

The record should include:

- Date the request was received.
- Name of the individual making the request.
- Nature and scope of the request.

- Whether identity verification was required.
- Details of any identity verification completed.
- Whether clarification was required.
- Details of any clarification requested or received.
- Applicable response deadline.
- Person responsible for managing the request.
- Actions taken to locate, review or correct relevant information.
- Details of any information withheld or redacted and the reason.
- Details of any extension to the response period and the reason.
- Date the final response was issued.
- Outcome of the request.
- Copies or references to relevant correspondence and supporting records.

Records will be retained in accordance with the BOOST Data Retention Schedule and access will be restricted to authorised personnel.

6.4 Identity Verification

BOOST may request reasonable evidence of identity where necessary to prevent personal information being disclosed to the wrong person.

Where a request is made on behalf of another individual, suitable evidence of authority to act on that person's behalf may also be required.

Only information reasonably necessary to verify identity should be requested.

6.5 Response Times

BOOST will respond to valid data subject requests without undue delay and normally within **one month of receipt**.

Where permitted by law, the response period may be extended by up to a further two months where the request is complex or multiple requests have been received.

Where an extension is required, the individual will be informed within the initial one-month period and provided with the reason for the extension.

6.6 Locating and Reviewing Information

Relevant information will be identified from systems and records that may reasonably contain information within the scope of the request.

Before disclosure, BOOST will review the information to identify:

- Information relating to other individuals.
- Confidential or legally privileged information.
- Information subject to a statutory exemption.
- Information outside the scope of the request.
- Information that requires redaction before release.

Personal information relating to another person will not be disclosed where this would be inappropriate or unlawful.

6.7 Fees

BOOST will normally respond to data subject requests without charge.

A reasonable fee may only be considered where permitted by applicable legislation, including where a request is manifestly unfounded or excessive or where additional copies are requested.

6.8 Other Rights Requests

Requests for correction, deletion, restriction, objection or other data protection rights will be referred to the Data Protection Lead.

The request will be assessed against:

- The nature of the information.
- The purpose and lawful basis for processing.
- Applicable legal or contractual retention requirements.
- Any relevant exemptions.
- The rights and interests of other persons.

The decision and action taken will be appropriately recorded.

6.9 Complaints

Individuals may raise a complaint with BOOST where they have concerns about the way their personal information has been handled.

Complaints may be made using the contact arrangements published within the relevant BOOST Privacy Notice or through another appropriate communication route.

The Data Protection Lead will ensure that:

- Complaints are acknowledged within 30 days of receipt.

- Appropriate steps are taken to investigate the matters raised without undue delay.
- Relevant facts, records and information are reviewed fairly and proportionately.
- The individual is kept appropriately informed of progress.
- The outcome of the investigation is communicated without undue delay.
- Reasons for significant decisions are recorded.
- Any corrective or improvement actions are identified and monitored where required.
- Suitable records of the complaint, investigation and outcome are retained.

Individuals may also complain to the Information Commissioner's Office and are not required to complete BOOST's internal complaints process before doing so.

7. Personal Data Breaches and Cyber Security Incidents

BOOST TA Ltd will respond promptly to suspected or confirmed personal data breaches and cyber security incidents to limit harm, protect information and systems, and meet applicable reporting requirements.

7.1 What Must Be Reported

Personnel must immediately report any suspected or confirmed incident involving:

- Personal information sent to the wrong recipient.
- Loss or theft of a device containing Company information.
- Loss of paper records.
- Unauthorised access to Company systems or accounts.
- Compromised passwords or login credentials.
- Phishing or suspected fraudulent communications.
- Malware or ransomware.
- Accidental deletion or loss of important information.
- Unauthorised disclosure of personal or confidential information.
- Information being accessed by an unauthorised person.
- Incorrect permissions allowing inappropriate access.
- Loss of availability of personal information where this may affect individuals.
- Any other suspected compromise of Company information or systems.

Personnel must not delay reporting because the full extent of the incident is not yet known.

7.2 Immediate Actions

Where safe and appropriate, immediate actions may include:

- Disconnecting an affected device from the network.
- Locking or remotely securing a lost device.
- Changing or resetting compromised passwords.
- Revoking unauthorised access.
- Recalling an incorrectly sent email where possible.
- Asking an unintended recipient to securely delete information.
- Preserving relevant evidence.
- Contacting IT support.
- Preventing further disclosure or loss.

Personnel must not delete evidence or attempt extensive technical investigation unless authorised to do so.

7.3 Reporting Route

Suspected incidents must be reported as soon as practicable to:

- The Data Protection Lead.
- The relevant Manager.
- IT support where a technical or cyber security issue is involved.

The initial report should include, where known:

- Date and time the incident was discovered.
- Name of the person reporting the incident.
- Description of what has occurred.
- Information, systems, devices or accounts affected.
- Individuals who may be affected.
- Whether personal data may have been accessed, disclosed, altered, lost or destroyed.
- Immediate action already taken.
- Any continuing or immediate risk.
- Further action or support required.

- Any relevant evidence, screenshots, emails or system information available.

The person reporting the incident should not delay notification because all information is not yet available. Further details can be provided as the incident is investigated.

7.4 Breach Assessment

The Data Protection Lead, supported by relevant management and technical personnel, will assess the incident.

The assessment will consider:

- What happened.
- When the incident occurred.
- When BOOST became aware of it.
- What information was affected.
- The sensitivity of the information.
- Approximate number of individuals affected.
- Whether information was encrypted or otherwise protected.
- Who may have received or accessed the information.
- The likelihood of misuse.
- Potential consequences for affected individuals.
- Actions already taken to contain the incident.
- Further action required.

7.5 Notification to the Information Commissioner's Office

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, BOOST will notify the Information Commissioner's Office where required.

Where notification is required, it will normally be made without undue delay and, where feasible, within **72 hours** of BOOST becoming aware of the breach.

Where all relevant information is not immediately available, information may be provided in stages where permitted.

7.6 Notification to Individuals

Where a personal data breach is likely to result in a **high risk** to the rights and freedoms of affected individuals, BOOST will inform those individuals without undue delay where required.

The communication should explain, in clear language:

- The nature of the breach.
- The likely consequences.
- Measures taken or proposed by BOOST.
- Any action the individual should take.
- How to obtain further information.

7.7 Breach Register

BOOST will maintain a record of personal data breaches, including incidents that do not require notification to the Information Commissioner's Office.

The breach record should include:

- Incident reference number.
- Date and time the breach was identified.
- Description of the incident.
- Categories of personal data or information affected.
- Individuals or categories of individuals affected.
- Likely consequences and level of risk.
- Risk assessment outcome.
- Immediate containment action taken.
- Further corrective or preventive action required.
- Whether notification to the Information Commissioner’s Office was required.
- Date and reference of any ICO notification.
- Whether affected individuals were required to be notified.
- Date and method of any notification to affected individuals.
- Relevant internal or external parties notified.
- Investigation findings.
- Lessons learned.
- Date the incident was formally closed.
- Name of the person responsible for closure.

The breach register will be maintained securely, with access restricted to authorised personnel, and retained in accordance with the BOOST Data Retention Schedule.

7.8 Cyber Security Incident Response

Where an incident involves Company IT systems, BOOST may also take action to:

- Isolate affected systems.
- Disable compromised accounts.
- Reset credentials.
- Preserve logs and technical evidence.
- Identify affected devices or systems.
- Restore information from secure backups.
- Apply security updates or configuration changes.
- Involve external IT or cyber security specialists.
- Notify clients or other affected parties where contractually or legally required.

7.9 Review and Corrective Action

Following a significant incident, BOOST will review:

- How the incident occurred.
- Whether existing controls were followed.
- Whether technical controls require improvement.
- Whether access permissions require amendment.
- Whether additional training is required.
- Whether procedures need to be revised.
- Whether similar risks exist elsewhere in the business.

Corrective actions will be recorded and monitored through to completion.

8. Data Sharing, Processors and International Transfers

BOOST TA Ltd will only share personal or confidential information where there is a legitimate business, contractual or legal reason to do so.

Information will not be shared more widely than necessary.

8.1 Internal Sharing

Personal information may be shared internally where required for legitimate business purposes.

Access will be limited to persons who need the information for their role.

This may include:

- Directors.
- Managers.
- HR or administration personnel.
- Project Managers.
- Health and safety personnel.
- Finance personnel.
- IT support.
- Other authorised personnel.

8.2 External Sharing

Information may be shared with external parties where appropriate, including:

- Clients.
- Principal Contractors.
- Professional advisers.
- Insurers.
- Payroll providers.
- IT and cloud service providers.
- Training providers.
- Occupational health providers.
- Government departments.
- Regulators.
- Emergency services.
- Other parties where required by law or contract.

Before sharing information, BOOST will consider:

- Whether there is a lawful basis.
- Whether the recipient genuinely requires the information.
- Whether the amount of information being shared is proportionate.
- Whether suitable security arrangements are in place.
- Whether a data processing agreement or other contractual control is required.

8.3 Data Processors

Where another organisation processes personal information on behalf of BOOST, BOOST will use suitable providers and apply appropriate contractual controls.

Where required, processor arrangements will address:

- Processing only on documented instructions.
- Confidentiality.
- Information security.
- Use of sub-processors.
- Assistance with individual rights.
- Assistance with breach management.
- Return or deletion of information at the end of the service.
- Audit or compliance information where appropriate.

8.4 Data Sharing Agreements

A formal data sharing agreement may be used where personal information is shared regularly or where the nature or sensitivity of the information warrants additional control.

The agreement may define:

- Purpose of sharing.
- Information to be shared.
- Lawful basis.
- Responsibilities of each party.
- Security requirements.
- Retention arrangements.
- Individual rights.

- Breach notification arrangements.
- Review and termination arrangements.

8.5 International Transfers

Where personal information is transferred outside the UK, BOOST will ensure that an appropriate lawful transfer mechanism is in place where required.

This may include:

- Transfer to a country covered by UK adequacy regulations.
- Use of an appropriate safeguard recognised under UK data protection legislation.
- Use of an applicable exception where legally permitted.

Before making a restricted transfer, BOOST will consider:

- The destination country.
- The recipient.
- The nature and sensitivity of the information.
- The transfer mechanism.
- Security arrangements.
- Any additional safeguards required.

8.6 Cloud and Online Services

Before using a cloud-based or online service to store or process personal or confidential information, BOOST will consider:

- Where information is stored.
- Security controls.
- Access controls.
- Backup arrangements.
- Data processing terms.
- Sub-processors.
- International transfers.
- Data deletion and account closure arrangements.

Only approved services should be used for Company information.

8.7 Disclosure Required by Law

BOOST may disclose personal information where required by law, court order, regulator or other lawful authority.

Where reasonably practicable, the disclosure will be limited to the information necessary to meet the requirement.

9. Training, Awareness and Compliance

BOOST TA Ltd will ensure that personnel who handle personal information or use Company systems understand the data protection and cyber security requirements relevant to their role.

9.1 Induction

Relevant personnel will receive appropriate information during induction covering:

- This Data Protection & Cyber Security Policy.
- Secure use of Company systems and devices.
- Password and multi-factor authentication requirements.
- Email and phishing awareness.
- Handling personal and confidential information.
- Reporting data breaches and cyber security incidents.
- Responsibilities when working remotely.
- Use of approved systems and applications.

9.2 Refresher Training

Data protection and cyber security awareness will be refreshed periodically and at least annually where appropriate.

Additional training may be provided following:

- Significant changes to systems or processes.
- Changes to legal or regulatory requirements.
- Introduction of new technology.
- Identification of recurring weaknesses.
- A significant data breach or cyber security incident.
- Changes to an individual's responsibilities.

9.3 Role-Specific Training

Personnel with additional responsibilities may require more detailed training.

This may include:

- Managers.
- Data Protection Lead.
- IT administrators.
- Personnel handling recruitment or employee records.
- Finance personnel.
- Persons responding to Subject Access Requests.
- Personnel responsible for incident or breach management.

9.4 Training Records

Where formal training is provided, BOOST will retain suitable records.

9.5 Personnel Responsibilities

Personnel must:

- Complete required training.
- Apply the controls described within this Policy.
- Raise questions where requirements are unclear.
- Report suspected weaknesses or insecure practices.
- Report incidents promptly.
- Cooperate with investigations where required.

9.6 Monitoring and Compliance

BOOST may review compliance with this Policy through:

- System and access reviews.
- Training records.
- Incident and breach records.
- Internal audits.
- Management review.
- IT security checks.

- Review of permissions and user accounts.
- Review of third-party service arrangements.

Significant non-compliance or recurring weaknesses will be investigated and appropriate corrective action taken.

9.7 Policy Breaches

Failure to comply with this Policy may expose BOOST, its clients or individuals to financial, legal, operational or reputational harm.

Where a breach of this Policy is identified, BOOST may:

- Remove or restrict system access.
- Require additional training.
- Introduce additional supervision or controls.
- Investigate the circumstances.
- Take appropriate disciplinary or contractual action where justified.
- Report matters to relevant authorities where legally required.

10. Records, ICO Registration and Policy Review

BOOST TA Ltd will maintain proportionate records to demonstrate compliance with its data protection and cyber security responsibilities.

10.1 Data Protection Records

Records may include:

- Privacy notices.
- Data processing agreements.
- Data sharing agreements.
- Subject Access Request records.
- Other individual rights requests.
- Personal data breach records.
- Cyber security incident records.
- Training records.
- Processor and service-provider information.
- Access and permission records.

- Retention arrangements.
- Data protection impact assessments where required.
- Records of significant data protection decisions.
- Relevant audit or review records.

10.2 ICO Registration and Data Protection Fee

BOOST TA Ltd will maintain registration with the Information Commissioner's Office and pay the applicable annual data protection fee where required under the Data Protection (Charges and Information) Regulations 2018.

The Data Protection Lead or nominated responsible person will ensure that:

- BOOST's ICO registration remains current.
- The applicable fee tier is reviewed where Company size or turnover changes.
- The annual fee is renewed when due.
- Registration details are updated where relevant Company information changes.
- Evidence of current registration and payment is retained.

The requirement will be reviewed if BOOST's processing activities materially change or where an exemption may become applicable.

10.3 Data Protection Impact Assessments

A Data Protection Impact Assessment will be considered before introducing processing that is likely to result in a high risk to individuals.

This may include:

- New technology involving significant personal data processing.
- Large-scale processing of particularly sensitive information.
- Significant monitoring of individuals.
- New systems involving extensive profiling or automated decision-making.
- Other processing identified as potentially high risk.

Where required, the assessment will identify:

- The proposed processing.
- Purpose and necessity.
- Risks to individuals.

- Existing controls.
- Additional safeguards required.
- Responsible persons.
- Approval and review arrangements.

10.4 Retention and Disposal Review

Retention arrangements will be periodically reviewed to ensure that:

- Information is not retained unnecessarily.
- Applicable legal and contractual requirements are met.
- Duplicate or obsolete information is removed where appropriate.
- Disposal methods remain secure.
- Information subject to an ongoing claim, investigation or legal requirement is retained where necessary.

10.5 Policy Review

This Policy will be reviewed at least annually and earlier where necessary following:

- Significant changes to data protection legislation or guidance.
- Significant changes to BOOST systems or technology.
- Introduction of new processing activities.
- Significant personal data breaches.
- Significant cyber security incidents.
- Audit findings.
- Changes to Company structure or responsibilities.
- Identification of weaknesses in existing controls.

10.6 Approval

Approved By: Giles Donovan & William Roberts
Position: Directors
Issue Date: 04 September 2026
Review Date: 03 September 2027
Document Reference: BOOST-GOV-POL-001

10.7 Revision History

Revision	Date	Description of Change	Prepared By	Approved By
01	04/09/2026	Initial issue.	Orakul Safety Ltd.	Giles Donovan & William Roberts