Thanet Computer Solutions Ltd

I.T Terms & Conditions

V.9.0

Please read this document carefully as it contains terms and conditions for our managed I.T services. We have made an effort to keep it clear and jargon-free!

Thanet Computer Solutions Ltd

Document Change Log

VERSION	AUTHOR	DATE	COMMENTS
V.6.0	Sam Bates	20/01/2026	Added SLA information to the bottom of the document
V7.0	Sam Bates	06/05/2026	Expanded and refined Terms & Conditions structure including service scope clarification, support and SLA enhancements, onboarding and offboarding provisions, security measures, commercial protections and general wording improvements.
V8.0	Sam Bates	16/07/2026	Clarified delay notifications, security service responsibilities, cloud backup scope, transition documentation, and cyber incident support and recovery exclusions.
V9.0	Sam Bates	22/08/2026	Clarified Microsoft 365 access responsibilities, monitoring scope, client governance duties, service exclusions, onboarding, cyber response, licensing, backups and SLA boundaries.

Thanet Computer Solutions Ltd

Contents

Thanet Computer Solutions Ltd ("we", "us", "our") provides managed IT services, support, consultancy, and related solutions to the customer ("you", "your", "client"). These Terms & Conditions form the basis of all services delivered unless otherwise agreed in writing.

1. Definitions

Managed Service Provider (MSP) – a proactive, ongoing IT management and support service delivered under a recurring fee model.

Service Agreement – the agreement outlining the services we provide, pricing, inclusions, exclusions, and support levels.

Devices – any endpoint, server, network component or cloud service under management (Only servers and endpoints are billable).

Best Endeavours – work carried out outside of working hours within a more flexible timeframe.

Authorised Contact – an individual nominated by the Client who has authority to request account, security, infrastructure or service changes on behalf of the Client.

2. General Disclaimer

2.1. By engaging us, you authorise Thanet Computer Solutions Ltd to manage, support, and maintain your IT environment.
2.2. All work is carried out professionally and with due care; however, specific results, recovery outcomes, or business impact improvements cannot be guaranteed.
2.3. Timeframes provided are estimates only and may vary.
2.4. IT work carries inherent risk, including system failure, data corruption, or data loss. You are responsible for ensuring appropriate backups exist unless backup services are included in your Service Agreement. Where backups are not in scope, we accept no responsibility for data loss, restoration, or business interruption.
2.5. You authorise us to install any required software, agents, monitoring tools, remote access software, or security protection necessary to deliver MSP services.
2.6. All remote support is subject to the same terms as onsite services.

3. Scope Of Managed Services

3.1. Services provided are defined in your Service Agreement and may include:
- Proactive monitoring and management
- Patching and updates
- Cybersecurity tools (AV/EDR, DNS filtering, MFA enforcement, etc.)
- Cloud services administration
- Helpdesk and user support
- Hardware lifecycle guidance and management

3.2. Proactive monitoring and management applies only to systems, devices, services and conditions that are expressly within the Service Agreement and capable of being monitored by the management, security or monitoring tools deployed by us. It does not constitute continuous manual supervision, auditing or inspection of the Client's entire IT environment.
3.3. Monitoring services rely upon automated tools, vendor integrations and configured alert thresholds. The existence of monitoring does not constitute a guarantee that every fault, security event, configuration change or abnormal condition will generate an alert or be detected.
3.4. The absence of an alert does not confirm that a system is functioning correctly, securely configured or free from faults. Monitoring systems are intended to assist service delivery and risk identification but cannot identify every failure, configuration issue, security weakness or operational risk.
3.5. Services are provided on a proactive basis, but not all issues can be predicted or prevented.
3.6. Requests falling outside the reasonable scope of the Service Agreement may incur additional charges.
3.7. We reserve the right to classify work as project activity where complexity, duration, planning requirements, risk, or resource demand exceeds standard support activity.

3.8. Examples of project activity may include migrations, office relocations, infrastructure redesign, major software deployments, server replacements, or onboarding activities involving significant planning or implementation work.

3.9. Devices not under a current agreement ("uncovered devices") are supported at ad hoc rates.

3.10. Physical servers may be classified separately from standard user devices and may be subject to a higher support rate due to their critical role and additional management requirements.

3.11. Servers host critical systems and data and therefore require appropriate backup and recovery solutions. Backup services are not included unless expressly stated in your Service Agreement and may incur additional costs. Where server backups are declined or not in scope, responsibility for data loss, restoration, and business interruption remains with you.

3.12. Backup integrity and successful restoration cannot be guaranteed unless recovery testing forms part of the Service Agreement.

3.13. The provision of backup services does not include disaster recovery, business continuity planning or guaranteed recovery time or recovery point objectives unless expressly stated within the Service Agreement.

4. Client Responsibilities

4.1. You must ensure users follow good security practice including:

- Strong unique passwords
- MFA wherever possible
- Not disabling or removing our monitoring or security agents
- Not installing unapproved software

4.2. You must provide remote access and necessary permissions for us to deliver services.

4.3. You must notify us of:

- New users, leavers, role changes
- New hardware, cloud services or business applications
- Changes to network infrastructure

4.4. The Client is responsible for notifying us promptly of starters, leavers, role changes and required access changes. We accept no responsibility for continued access resulting from delayed, incomplete or incorrect instructions from the Client.

4.5. Unless expressly included as a managed identity or access governance service, we are not responsible for independently identifying users who have left the organisation, changed roles or no longer require access.

4.6. Delays caused by unavailable Client personnel, lack of access, missing credentials, delayed responses, unavailable third parties or suppliers, incomplete information, or issues within the Client's systems, premises or operating environment may affect delivery timeframes and shall not constitute a failure to provide the Services or a breach of any service level, provided that the Provider notifies the Client as soon as reasonably practicable after becoming aware that such an issue is causing, or is likely to cause, a

material delay, and provides reasonable details of the issue and its expected impact where known.

4.7. You must ensure licensing, warranties and subscriptions remain valid where not managed by us.

4.8. Where we administer licensing on the Client's behalf, the Client remains responsible for providing accurate user requirements, approving applicable charges and notifying us of changes affecting licence requirements.

4.9. We are not responsible for determining whether licences meet the Client's legal, regulatory or software compliance obligations unless expressly engaged to provide a software licensing audit or consultancy service.

4.10. You are responsible for compliance with relevant laws and industry standards unless otherwise stated.

4.11. The Client remains responsible for identifying the legal, regulatory, contractual and industry requirements applicable to its business. Our provision of IT services does not constitute legal, regulatory, compliance or data protection advice unless expressly agreed.

4.12. You authorise us to create, modify, suspend and remove user accounts, access rights, devices and cloud services upon instruction from nominated authorised contacts.

4.13. Requests affecting accounts, permissions, infrastructure, security settings, financial matters or business critical systems may only be accepted from nominated authorised contacts.

4.14. The Client retains responsibility for all business decisions concerning user access, authority levels, data ownership and the appropriateness of access granted to individual users. We are not responsible for determining whether an employee, contractor or other individual has a legitimate business requirement for particular access.

5. Limitation Of Liability

5.1. We will not be liable for:

- Loss of business, loss of profits, revenue, goodwill, anticipated savings, or any indirect or consequential loss.
- Data loss caused by user actions, malware, hardware failure, corruption, or lack of adequate backups where backup services are not included within the Service Agreement.
- Breaches caused by weak passwords, insecure behaviour, disabled or declined security recommendations, or unapproved system changes.
- The Client is responsible for actions performed by its users, administrators and authorised third parties, including changes made directly within Microsoft 365 or other managed platforms without our involvement.
- Issues arising from third party suppliers, internet service providers, cloud platforms, or software vendors.
- Business interruption, service downtime, or losses arising from cyber incidents, ransomware, denial of service attacks, or outages affecting third party platforms or infrastructure providers.

5.2. Services relying upon third party suppliers, internet providers, cloud platforms, datacentres, software vendors, telecom providers, distributors or licensing providers are delivered subject to the availability and performance of those providers. We accept no liability for failures, interruptions, delays, security incidents or outages beyond our reasonable control.

5.3. Subject to clause **5.4**, our total aggregate liability arising from or in connection with the Services shall not exceed the total fees paid by the Client during the twelve months immediately preceding the event giving rise to the claim.

5.4. Our total aggregate liability arising from breaches of confidentiality, data protection obligations, or personal data processing in connection with the Services shall not exceed two times the total fees paid by the Client during the twelve months immediately preceding the event giving rise to the claim.

5.5. Nothing in these terms limits or excludes liability for fraud, fraudulent misrepresentation, death or personal injury caused by negligence, or any liability that cannot legally be limited or excluded under the laws of England and Wales.

6. Microsoft 365 & Cloud Services

6.1. Cloud services are provided under Microsoft's terms, which take precedence.

6.2. Customers must sign the Microsoft Cloud Agreement before onboarding.

6.3. Administrative access may be required for us to administer agreed Microsoft 365 services and implement security controls included within the Service Agreement.

6.4. We will not access mailbox content except where reasonably necessary to deliver an authorised service, investigate a reported issue or perform work instructed by an Authorised Contact.

6.5. Cloud services do not replace the need for backups; unless a cloud backup solution is included in your agreement, you accept responsibility for data loss due to deletion, ransomware or user error.

6.6. Microsoft does not guarantee one hundred percent uptime.

6.7. Unless expressly included within the Service Agreement, we are not responsible for routinely auditing, reviewing or monitoring user access rights, mailbox permissions, mailbox delegation, shared mailbox membership, Microsoft 365 group membership, SharePoint permissions, Teams membership or other access permissions within the Client's cloud environment.

6.8. Responsibility for determining which individuals should have access to systems, data, mailboxes and other resources remains with the Client. We will implement, amend or remove permissions following instructions from a nominated Authorised Contact.

6.9. The Client is responsible for notifying us promptly of changes in employment, responsibilities, roles or other circumstances requiring access permissions to be amended or removed. Unless specifically agreed otherwise, we are not responsible for identifying inappropriate, excessive, historic or no longer required permissions.

7. Security & Cyber Protection

7.1. We may deploy Webroot or equivalent enterprise cyber security solutions.
7.2. Responsibility for system protection remains with the Client except to the extent that specific security services are expressly included within the Service Agreement.
7.3. If recommended security measures are declined, responsibility for resulting breaches rests entirely with you.
7.4. We reserve the right to suspend or limit services where system security, malware activity, compromised accounts or unmanaged risks may negatively affect our infrastructure, staff or other clients.
7.5. We may recommend and, where agreed or included within the Service Agreement, implement reasonable security controls including MFA, Conditional Access policies, device encryption, privilege separation and endpoint restrictions.
7.6. The provision of managed IT or security services does not constitute a guarantee that the Client's environment complies with every vendor recommendation, security framework, regulatory requirement, cyber insurance condition or industry best practice unless a specific compliance or auditing service has been expressly agreed.

8. Remote Support & Access

8.1. Remote access tools are used for both attended and unattended support.
8.2. Unattended access and automated monitoring tools may be enabled under our agreement to assist with proactive support, alerting and incident response. Monitoring is primarily automated and does not constitute continuous human supervision or a 24 hour security operations service unless expressly included within the Service Agreement.
8.3. We will not access systems unnecessarily or without legitimate operational reason.
8.4. Clients must not remove or alter remote access tools without written agreement.
8.5. Removal, interference with or restriction of monitoring and remote access tools may affect service delivery, response times and security protections.
8.6. Alerts are reviewed and acted upon in accordance with the applicable support arrangements and service hours. Monitoring cannot guarantee detection of every failure, security event or abnormal condition.

9. Privacy, Data & GDPR

9.1. We maintain appropriate technical and organisational measures intended to protect personal data processed in connection with the Services.
9.2. Temporary data copies may be taken only where required and deleted after use.
9.3. Incidental data visibility may occur during IT work; you remain responsible for storing confidential documents securely.
9.4. Credentials stored by us are encrypted and protected by MFA.
9.5. Full details are found in our published Privacy Policy.

10. Confidentiality & Non Disclosure

10.1. We treat all client information confidentially.
10.2. A separate NDA can be provided if required.

11. Intellectual Property

11.1. Documentation, scripts, templates, automation routines, monitoring policies, deployment methods and internal operational processes developed by us remain our intellectual property unless otherwise agreed in writing.
11.2. Client specific documentation, credentials, tenant information and configuration data created specifically for the Client remain the property of the Client.
11.3. Upon termination and settlement of all outstanding payments, we will provide the Client or its nominated incoming provider with the client specific documentation and credentials held by us that are reasonably necessary for an orderly transfer of services. This may include relevant credentials, asset and licensing information, supplier details and available configuration documentation. It does not include our intellectual property described in clause 11.1 or the creation of extensive new or bespoke documentation. Additional transition work will be handled in accordance with clause 14.4.

12. Non Solicitation

12.1. During the term of the agreement and for twelve months following termination, the Client shall not directly or indirectly solicit, recruit, engage or employ our employees or contractors involved in delivering services without prior written agreement.
12.2. If this occurs, the Client agrees to pay a recruitment fee equal to six months of the individual's gross annual salary.

13. Service Delivery & Support

13.1. Support is provided professionally during standard support hours of Monday to Friday, 08:30 to 17:30 excluding public holidays unless otherwise agreed within the Service Agreement.
13.2. Escalation to onsite support occurs when remote resolution is not feasible.
13.3. Parts and labour are warranted for fourteen days unless otherwise stated.
13.4. We do not guarantee that upgrades will extend hardware lifespan.
13.5. Equipment left for over three months may be recycled or disposed of.
13.6. Suitable operational cover will be maintained to support continuity of service during staff absence, annual leave or unforeseen circumstances.
13.7. Service levels, including response and resolution targets, are defined in our Service Level Agreement (SLA), which forms part of these Terms where applicable.
13.8. Onsite support is chargeable unless explicitly included in your Service Agreement and is subject to availability, travel time, and our prevailing hourly rates.

13.9. We reserve the right to refuse, postpone or suspend services where abusive behaviour, unlawful activity, unsafe working environments, security concerns or risks to staff welfare exist.

14. Onboarding & Offboarding

14.1. Standard onboarding associated with commencement of a managed service agreement does not normally attract a separate onboarding fee. Complex migration, remediation, discovery, documentation or implementation work required during onboarding may be treated as project activity and separately chargeable.

14.2. Offboarding requires thirty days' notice and includes:

- Removal of agents
- Transfer of credentials (where appropriate)
- Documentation handover
- Disabling our administrative access

14.3. Final invoices must be paid before offboarding is completed.

14.4. Offboarding activity exceeding two hours, project style transition work, third party liaison, infrastructure migration support, or documentation creation requested specifically for transition purposes may be chargeable at our prevailing rates.

14.5. We will provide reasonable assistance during transition; however, no obligation exists to redesign, rebuild or reconfigure systems for incoming providers.

15. Payment Terms

15.1. Payment is due within fourteen days of invoice.

15.2. Non payment may result in suspension or restriction of support services, remote access tools, monitoring systems, licences, cloud services, security products, managed services and associated products until payment is received.

15.3. Suspension shall not relieve the Client of payment obligations during the suspension period.

15.4. Service plans are billed monthly in advance (or annually if agreed).

15.5. Ad hoc services are billed separately in arrears on the last day of the month.

15.6. We reserve the right to charge statutory interest and debt recovery costs on overdue invoices in accordance with applicable legislation.

16. Hardware & Software Supply

16.1. Hardware, software licences, cloud subscriptions and special order items are non cancellable and non returnable once ordered unless faulty or otherwise required under applicable law.

16.2. Warranty terms follow those of our suppliers and manufacturers.

16.3. Large hardware orders may require upfront payment.

16.4. Risk in supplied equipment transfers to the Client upon delivery or confirmed receipt.
16.5. The Client remains responsible for costs incurred where equipment, licensing, subscriptions or supplier commitments have already been ordered or provisioned.

17. Service Exclusions

17.1. Unless stated in your agreement, the following are not included:

- Project work (migrations, server builds, Wi Fi redesign and similar activities)
- Major infrastructure changes
- Bespoke development
- Unsupported legacy systems
- Line of business software support (beyond liaison with vendor)
- Data recovery services
- Hardware failure beyond basic troubleshooting
- Recovery from ransomware or cyber attack

Recovery from ransomware or a cyber attack requiring extensive remediation, forensic investigation, specialist third party services, data recovery or significant system rebuilding, unless expressly included within the Service Agreement. Where reasonably practicable, we may provide initial technical assistance to help identify and contain a suspected cyber incident. Extensive investigation, forensic analysis, remediation, recovery, reporting, legal or regulatory assistance and specialist incident response services are outside normal managed support unless expressly agreed.

We are not responsible for monitoring the internal operation, configuration, data integrity, permissions, security or business processes of third party or line of business applications unless expressly included within the Service Agreement.

17.2. We reserve the right to refuse or limit support for operating systems, hardware, applications or infrastructure that are end of life, unsupported by their manufacturer, or present operational or security risks.
17.3. We do not guarantee compatibility, performance or supportability of software, hardware or systems supplied by third parties unless specifically agreed within the Service Agreement.

18. Price Changes

18.1. Prices may change upon not less than thirty days written notice.
18.2. Pricing may also change if:

- Device count increases or decreases
- Licensing or vendor costs increase
- Service scope expands

18.3. As part of normal service operation, pricing is reviewed annually. Any adjustment will typically take place once per year and will reflect changes in operating costs, staffing, tooling, security requirements, and supplier pricing. We will always provide not less than thirty days written notice of any pricing adjustment.

19. Termination Of Contract

19.1. Unless otherwise specified in the Service Agreement, services are supplied on a rolling monthly basis and may be terminated by either party with thirty days written notice.
19.2. Where services are provided under a fixed term agreement, the Initial Term shall be defined within the Service Agreement.
19.3. Following expiry of the Initial Term, services shall automatically continue on a rolling monthly basis unless otherwise agreed in writing.
19.4. If the Client terminates a fixed term agreement before expiry of the Initial Term, the Client shall remain liable for fees due for the remainder of the agreed term less any direct cost savings reasonably achieved by us as a result of the early termination.
19.5. The Client shall also remain liable for any non cancellable supplier commitments, licence costs, hardware procurement costs or third party charges incurred by us.
19.6. All outstanding invoices become immediately payable upon termination.

20. Force Majeure

20.1. Neither party shall be liable for delays or failures resulting from circumstances outside reasonable control including supplier failures, internet outages, utility interruption, cyber incidents, natural disasters, acts of government, industrial disputes, telecommunications failures or other unforeseen events.
20.2. Where such circumstances continue for a prolonged period, either party may terminate the affected services upon reasonable written notice.

21. Changes To Terms & Conditions

21.1. These Terms and Conditions may be updated from time to time.
21.2. Clients will be notified of material changes by email.
21.3. Updated terms will take effect no earlier than thirty days from notification and will not apply retrospectively. Continued use of services after the effective date constitutes acceptance.

22. Governing Law

22.1. These Terms and Conditions and any dispute or claim arising from them shall be governed by and interpreted in accordance with the laws of England and Wales.
22.2. The courts of England and Wales shall have exclusive jurisdiction.

Service Level Agreement (SLA)

Scope of Services

We will deliver IT support services in accordance with the service levels defined in this Agreement. All support requests ("Tickets") will be prioritised and managed based on their impact and urgency.

Support Hours

Standard support is provided during the following hours:

- Monday to Friday: 08:30 to 17:30 (excluding public holidays)

Support requests submitted outside of these hours will be addressed on the next business day unless otherwise agreed in writing. Out of hours support may be provided on a best effort basis and may be subject to additional charges.

Incident Priority Levels

Incidents will be classified as follows:

- **Priority 1 (Critical):** Complete loss of service affecting the Client's business operations (e.g. server outage, network failure)
- **Priority 2 (High):** Significant service degradation or multiple users affected
- **Priority 3 (Medium):** Issue affecting a single user or non-critical function
- **Priority 4 (Low):** Service requests, minor issues, or general enquiries

We reserve the right to assign and adjust priority levels based on available information.

Target Response and Resolution Timeframes

We will use reasonable endeavours to meet the following targets:

Priority	Response Time	Target Resolution
Priority 1	Within 15 - 30 minutes	4 to 8 business hours
Priority 2	Within 1 hour	Within 1 business day
Priority 3	Within 4 business hours	1 to 3 business days
Priority 4	Within 1 business day	As scheduled

Service targets are objectives only and do not constitute guaranteed service credits, contractual penalties or warranty obligations.

Response time is defined as the time taken to acknowledge the Ticket and begin initial investigation.

Resolution time is defined as the time taken to resolve the issue or implement a reasonable workaround.

Service Delivery

We will make commercially reasonable efforts to resolve all incidents within the target timeframes. However, resolution times are not guaranteed and may be affected by factors including but not limited to:

- Third party supplier delays
- Hardware failure requiring replacement
- Client availability or delays in providing required information
- Complexity of the issue

Planned maintenance, upgrades and emergency security activity may occur outside standard support hours where reasonably necessary.

Client Responsibilities

The Client agrees to:

- Report incidents promptly via the agreed support channels
- Provide accurate and complete information when logging Tickets
- Ensure authorised personnel are available to assist with troubleshooting where required
- Maintain supported systems in accordance with our recommendations

Exclusions

This SLA does not apply to:

- Issues caused by third party services, vendors or infrastructure outside our control.
- Unsupported systems or software
- Client induced faults or unauthorised changes
- Scheduled maintenance periods (where notified in advance)
- Time during which a Ticket is awaiting information, approval, access, testing or action from the Client or a third party does not count towards target resolution timeframes.

Escalation

Where an issue cannot be resolved within the expected timeframe, it will be escalated internally and, where necessary, to relevant third party vendors.

Review and Amendments

We reserve the right to review and amend this SLA from time to time. Any material changes will be communicated to the Client in writing.