TERMS AND CONDITIONS

Managed IT Services | Microsoft 365 | Cybersecurity | Online Store

Office Logics Equipment Ltd (Trading as "OLE – Our Local Experts")

Last updated: May 2026

1. Scope of Services

OLE provides, including but not limited to:

- Managed IT Services
- IT support and consultancy
- Cloud services (including Microsoft 365)
- Cyber security services
- IT hardware, software and licensing
- Implementation and project services

The exact scope of services provided will be defined in:

- An accepted quote or proposal
- A service schedule
- A managed services agreement
- An online order confirmation

2. Online Store & Quotes

Orders placed via OLE's online ordering platform (including Kaseya Quote Manager) are subject to these Terms.

- All quotes are valid for 30 days, unless stated otherwise
- Prices exclude VAT unless specified
- Product availability is subject to supplier stock
- Acceptance of a quote constitutes a binding agreement

OLE reserves the right to correct pricing or clerical errors prior to acceptance.

3. Managed IT Services

Where the Customer subscribes to Managed IT Services:

- Services are delivered during agreed support hours

- Support is provided remotely unless otherwise agreed
- On-site visits may incur additional charges (or may be included in the agreed package, subject to fair usage)
- Out-of-scope work will be quoted separately

OLE does not guarantee uninterrupted service and shall not be liable for:

- Third-party failures
- Internet or power outages
- Vendor or manufacturer issues
- Pre-existing system faults

4. Customer Responsibilities

The Customer agrees to:

- Provide accurate and complete information
- Maintain licensed and supported software
- Ensure suitable backups are in place (unless provided by OLE)
- Follow reasonable security recommendations

OLE is not responsible for issues caused by:

- Unsupported or unlicensed software
- Customer-initiated changes
- Third-party access without our authorisation

5. Hardware, Software & Licensing

- Hardware warranties are provided by the manufacturer
- Software and cloud licences remain governed by the vendor's terms
- Licensing misuse or non-compliance is the Customer's responsibility

OLE acts as a reseller or facilitator and is not liable for vendor policy changes or pricing updates.

6. Fees & Payment Terms

- Invoices are payable within 14 days unless otherwise agreed
- Late payments may result in service suspension
- Interest may be applied in accordance with Irish law

OLE reserves the right to withhold services where accounts are overdue.

7. Data Protection & GDPR

OLE acts as:

- A Data Processor when providing IT services
- A Data Controller for its own business operations

We process personal data in accordance with:

- GDPR
- Irish Data Protection legislation

Further details are available in our Privacy Policy.

8. Confidentiality

Both parties agree to treat confidential information as strictly confidential, including:

- Business information
- Network details
- Login credentials
- Commercial terms

This obligation survives termination of services.

9. Limitation of Liability

To the fullest extent permitted by Irish law:

- OLE shall not be liable for indirect or consequential losses
- Total liability shall not exceed the fees paid by the Customer in the preceding 12 months

Nothing limits liability for death, personal injury, or fraud.

10. Termination

Either party may terminate services:

- With written notice per the agreed contract
- Immediately in the event of material breach

Upon termination:

- All outstanding invoices become due
- Access to systems managed by OLE may be removed

- Data handover is chargeable unless agreed otherwise

11. Force Majeure

OLE is not liable for delays or failures caused by events beyond reasonable control, including:

- Acts of God
- Power or network outages
- Third-party supplier failures

12. Governing Law

These Terms are governed by the laws of Ireland, and the Irish courts shall have exclusive jurisdiction.

13. Entire Agreement

These Terms, together with:

- Accepted quotes
- Service schedules
- Managed services agreements

constitute the entire agreement between the parties.

14. Contact

For questions relating to these Terms:

Email: support@ole.ie

Website: www.ole.ie

Schedule A – Service Schedule (Operational Terms)

A1. On-Boarding

Prior to commencement of the Services, OLE will on-board the Client's IT infrastructure:

- Review and, if necessary, advise the Client of changes to the IT Equipment configuration required to ensure the Services can be delivered effectively (including protective services such as anti-virus software and backup software).
- Install Monitoring Agents and anti-Malware software and inform the Client if OLE is unable to configure any IT Equipment to provide necessary alerting; OLE will agree a suitable alternative with the Client.

- Document the Client IT Infrastructure architecture in IT Glue.

A2. Helpdesk

Subject to fair usage, there are no restrictions on the number of Incidents that the Client can report to OLE's Helpdesk. OLE's Helpdesk provides support and assistance in the use of IT Equipment and/or Hosted Services, including:

- Management of prompt resolution of Incidents within IT Equipment and/or Hosted Services identified by the Client.
- Provision of help and guidance in the use and configuration of IT Equipment and/or Hosted Services.
- Remote access to facilitate Incident resolution where possible and appropriate.
- Escalation management where required in the event of protracted Incident resolution.
- Third-party vendor liaison where required (Plus and Premium only).

In the first instance, OLE will endeavour to resolve Incidents remotely. However, if OLE determines that an on-site visit is either necessary or the most efficient manner to resolve an Incident, OLE will dispatch an engineer to the Client's site and will not unreasonably delay dispatch.

Subject to fair usage in Helpdesk Plus and Premium packages, there are no restrictions on the number of on-site visits OLE will make where remote resolution is not possible. Clients on Helpdesk Essentials will be quoted in advance for on-site support or may have this covered using a Block of Time Agreement.

The Client may raise Incident reports by one of the following methods:

- If the Client subscribes to a Complete or Enhanced Security Service Package, via the OLE App (where applicable).
- By email to OLE Helpdesk: support@ole.ie
- By telephone to OLE Helpdesk during business hours.

The Helpdesk is available during the Hours of Cover: 8:00am to 6:00pm Monday to Friday, excluding bank and public holidays.

OLE shall aim to make an initial response to the Client request for assistance within thirty (30) minutes of the Client raising the Incident report and shall use reasonable endeavours to resolve the Incident.

When reporting an Incident, the Client should provide:

- Name of Client and person reporting the Incident
- Contact telephone number
- Description of the Incident
- Description of actions taken prior to the Incident occurring
- Explanation of how the Incident has been diagnosed
- Any other relevant information

A3. Service Level Agreement (Helpdesk)

OLE Helpdesk SLA targets are set out below. This SLA covers standard working hours only. Emergency and out-of-hours cover is subject to Best Effort response times only.

Trouble	Priority	Response time	Resolution time
Service not available (all users and functions unavailable)	1 = Critical	15 mins	ASAP – Best Effort
Significant degradation of service (large number of users or business critical functions affected)	2 = High	30 mins	ASAP – Best Effort
Limited degradation of service (limited number of users or functions affected; business process can continue)	3 = Normal	Within 2 hours	ASAP – Best Effort
Small service degradation (business process can continue; one user affected)	4 = Scheduled	Within 8 hours	ASAP – Best Effort

OLE shall make reasonable endeavours to meet these targets. Failure to meet these targets shall not be deemed a breach of the Agreement.

A4. Complaint Handling (Operational)

If dissatisfied with any Services-related matter, the Client should make a complaint using the following escalation path. If the complaint remains unresolved, the Client should escalate to the next level in the path:

- Email: support@ole.ie
- If further escalation is required, request escalation to OLE Operations Team via support@ole.ie or telephone.
- If further escalation is required, request escalation to OLE Senior Management via support@ole.ie or telephone.

Formal complaints can be made by email or telephone, and will be responded to within three (3) Working Days.

A5. Standard Operating Procedures

Drawing on experience of supporting business-critical IT infrastructure, OLE maintains technology standards addressing technology, usage, and compliance. OLE will regularly evaluate the Client IT Infrastructure against these standards and identify misalignments. These are communicated through periodic Strategic Business Reviews.

OLE will work alongside the Client to develop and maintain Client-specific standard operating procedures to assist with management of business-as-usual changes including new starters, leavers and data management.

A6. IT Documentation & Runbook

OLE will maintain documentation of the IT Infrastructure, identify the roles of each component and, on request, provide the Client with a copy of documentation. Documentation includes:

- Password Documentation: system administrative passwords recorded and held securely in encrypted format by OLE.
- Relevant configuration data.

A7. Proactive Threat and Breach Detection

Endpoint Detection and Response (Plus and Premium): OLE provides ransomware detection using monitored ransomware canaries. On detection of a potential security incident, an investigation is invoked by a team of security experts to confirm whether changes indicate infection or malicious encryption and to assist remediation of cyber threats, including persistent footholds where identified.

External Vulnerability Monitoring: OLE monitors open firewall and router ports for potential security exposure (e.g., RDP, file sharing, SQL services). Reports identify scanned IPs, protocols, ports, last query time, and (where available) detected services. This provides visibility to ensure ports are open securely and appropriately.

A8. Monthly Usage Report

OLE will provide the Client with a Monthly Executive Report providing an overview of service usage by user, device and licensed mailbox. This is used to support monthly billing.

A9. Server Monitoring and Management

Key server monitoring items include:

- Critical Event Logs
- C:\ and other drives space > 90% usage
- CPU time and/or memory usage > 90%
- Mission critical software not running
- Email outages
- Server outages
- Hardware management errors (where applicable)
- Backup failures

A10. Desktop Monitoring and Management

Key workstation monitoring items include:

- C:\ disk space > 90% usage
- RAM usage
- Anti-virus updates
- Patch updates – Windows and Microsoft Apps

A11. Site Monitors

Key site monitoring items include:

- Patching levels
- Antivirus definition dates
- Defragmentation status (where applicable)
- SMART / disk errors
- Antivirus disabled/missing
- Blacklisted software present
- New software installed
- Site / firewall offline

- New computers detected
- Device health and remote wipe
- Microsoft 365 security monitors

A12. On-Site Support

OLE will endeavour to resolve Incidents remotely first. Where OLE determines an on-site visit is required, OLE will dispatch an engineer and will not unreasonably delay dispatch. For Helpdesk Essentials, on-site support requires a quote or Block of Hours coverage. On-site visits are included under Plus and Premium plans (subject to fair usage).

On-site visits will be made during the Working Day.

A13. Asset and Inventory Report

Using Server and Endpoint Monitoring Agents, OLE will compile and maintain an asset register for the Client IT Equipment estate, including hardware and software inventories. Asset reports will be made available to the Client on request.

A14. Advanced Security Awareness Training and Phish Testing

OLE's Advanced Security Awareness Training is targeted at increasing End User awareness of cybersecurity threats and mitigations. Where included, OLE provides:

- Access to a wide range of cyber training materials for End Users
- Automated training campaigns and scheduled email reminders
- Phish testing/simulations and reporting (where applicable)

A15. Email, Teams, SharePoint and OneDrive Backup (Microsoft 365)

OLE's Backup Service for Microsoft 365 protects the Client against loss of data held within Microsoft cloud infrastructure, including loss due to user error or subscription expiry. OLE will back up Microsoft 365 data based on the number of End Users and storage capacity set out on the Quote.

Microsoft 365 backups include:

- OneDrive file and folder data backups (documents) per End User
- Exchange data including emails, attachments, notes, deleted items, contacts (excluding photographs), tasks and calendar events (including attendees, recurrence, attachments and notes)
- SharePoint site collections (primary, custom, group and team) including folders, libraries, sets, site assets, templates and pages
- Groups (including conversations, plans, files, sites and calendar)

- Teams (including wiki and chat)

Backups can be configured to run automatically or on-demand. The Backup and Recovery Service is fully managed by OLE. The backup system will automatically notify OLE of backup success or failure. Backups are encrypted at rest and during transmission. Backup data will be retained for 1 year.

Data restoration:

- Data restores will only be initiated by OLE when requested by an authorised representative of the Client
- OLE will use reasonable endeavours to restore data at the level of granularity requested by the Client (image, directory or file level where applicable)
- OLE will use reasonable endeavours to restore data to the location specified by the Client

Whilst OLE executes automatic backups and monitors backup performance 24×7×365, OLE will carry out the following during Hours of Cover:

- Respond to Client requests for data restores
- Respond to and investigate Incidents that arise in the service which cannot be remediated automatically, whether raised by the Client or by OLE monitoring agents

Test Data Restore: At the Client request, OLE can perform occasional test restores of backed-up data to validate backups. OLE will agree a test target (e.g., mailbox or SharePoint site) and perform the test restore at an agreed time. Test restores are chargeable at OLE's prevailing rate.

A16. After Hours Support

After Hours Support provides:

- 24×7 response to and, where possible, remediation of Incidents identified by OLE monitoring systems
- 24×7 Helpdesk support for response and remediation of Critical and High priority Incidents raised by the Client
- Application of patches and associated equipment reboots outside of Working Hours