CORRESPONDENCE ADDRESS
1 YEWDALE CRESCENT
WIGAN
LANCASHIRE
WN1 2HP

WORKSHOP
UNIT 2
TOWNSEND FARM
RUFFORD ROAD
BISPHAM
MAWDESLEY
L40 3SA

TELEPHONE: 01257 464601
EMAIL: OFFICE@LOST-ART.CO.UK
WEB: WWW.LOST-ART.CO.UK

LOST ART LIMITED: CYBER SECURITY POLICY

1. Purpose

This policy sets out how Lost Art Limited protects its information, systems and services from cyber security threats. It defines minimum controls to maintain confidentiality, integrity and availability, support business continuity, and meet applicable UK legal, regulatory and contractual obligations (including data protection).

2. Scope

- This policy applies to all employees, contractors and temporary staff who access **[Organisation name]** information or systems.
- It covers all devices and services used to store, process or transmit organisational information (including laptops, mobiles, servers, cloud services, networks and removable media).
- Third parties with access to organisational information must meet the relevant requirements in this policy and any supplier security terms.

3. Key definitions

- **Information asset**: Data, systems, services or devices that have value to the organisation.
- **Personal data**: Any information relating to an identified or identifiable individual.
- **Incident**: An event that compromises (or may compromise) confidentiality, integrity or availability, including suspected phishing, malware, unauthorised access, loss of device, or data breach.

4. Roles and responsibilities

- **Managing Director (Dominic Liptrot)**: sets risk appetite; approves this policy; ensures appropriate funding and oversight.
- **Information Security Lead/ Data Protection Officer/Privacy Lead** (Damian Liptrot): maintains security controls; manages risk and incidents; reports on security performance.
- **All users**: follow this policy, complete training, and promptly report suspected incidents.

5. Policy requirements (minimum controls)

Controls in this section represent the minimum baseline expected across the organisation. Additional controls may be required based on risk assessments, system criticality, and contractual/regulatory requirements.

5.1 Asset management and secure configuration

- Maintain an up-to-date inventory of in-scope devices, key systems and cloud services (owner, purpose, location, criticality).
- Use secure baseline configurations (hardened build) for endpoints, servers, network devices and cloud services.
- Remove or disable default accounts and unnecessary services; change default passwords; restrict administrative interfaces.
- Use approved software only; block or restrict unauthorised software installation where feasible.

5.2 Access control and authentication

- Grant access on a least-privilege basis and review access periodically.
- Use unique user accounts; shared accounts are prohibited except where formally approved and technically controlled.
- Admin access must use separate privileged accounts where practical.
- Multi-factor authentication (MFA) must be enabled for remote access and for cloud services where available, especially email and administrative access.
- Passwords (where used) must be strong and not reused across systems; passwords must never be shared or written in unsecured locations.

5.3 Network security and firewalls

- Use boundary firewalls and/or secure network gateways to control inbound and outbound traffic.
- Endpoints must have host firewalls enabled, with rules configured to reduce exposure.
- Remote access must be secured (e.g., VPN or secure zero-trust access) and protected with MFA.

- Wi-Fi must be secured using strong encryption and separate guest access where required.

5.4 Malware protection

- All endpoints and servers must use supported anti-malware controls (e.g., endpoint protection) with automatic updates enabled: Note: we currently isolate all devices rather than network but this element of the policy will apply if we network devices in the future.
- Email and web filtering should be used where feasible to reduce phishing and malware delivery.
- Users must not disable or bypass security tooling.

5.5 Vulnerability and security update management

- Apply security updates for operating systems, firmware and applications in a timely manner, prioritising critical and high-risk patches.
- Unsupported (end-of-life) operating systems and applications must not be used for organisational processing unless an exception is approved with compensating controls.
- Regularly scan for vulnerabilities where appropriate to the organisation's size and risk.

5.6 Data protection, classification and handling

- Information must be handled in accordance with its sensitivity (e.g., Public, Internal, Confidential).
- Personal data must be processed securely using appropriate technical and organisational measures, consistent with UK GDPR obligations.
- Encrypt devices and removable media where feasible, especially when storing Confidential information or personal data.
- Only approved storage locations/services may be used for business data. Personal email and unapproved cloud storage must not be used for business data.
- Data must be securely disposed of in line with retention requirements (e.g., secure wipe, shredding).

5.7 Backup, recovery and resilience

- Back up critical systems and data regularly, including configuration where relevant.
- Protect backups from ransomware (e.g., offline/immutable backups and separate credentials) and limit access.
- Test restores on a defined schedule to ensure recovery is achievable within business requirements.

6. Incident management and reporting

All users must report suspected incidents immediately (e.g., phishing emails, lost devices, suspicious logins, malware alerts, mis-sent emails containing personal data). Rapid reporting reduces harm.

1. **Report**: Contact **Damian Liptrot (damianlostart@hotmail.co.uk/07947325557** immediately and preserve evidence (do not delete suspicious emails).
2. **Triage**: Damian to assesses severity, scope and potential personal data impact.
3. **Contain**: Isolate affected devices/accounts; reset credentials; block malicious indicators.
4. **Eradicate and recover**: Remove malware, restore from backups, apply fixes.
5. **Learn**: Document root cause, corrective actions, and update controls/training.

If an incident involves (or is likely to involve) a **personal data breach**, Damian must be engaged immediately to assess notification obligations and timelines, and to coordinate any required communications.

7. Supplier and third-party security

- Security requirements must be assessed before onboarding new suppliers who will access organisational systems or data.
- Contracts must include appropriate security and data protection clauses (including incident notification timeframes).
- Access for suppliers must be time-bound, least-privilege, and reviewed regularly.
- Suppliers must not further subcontract access to organisational data without written approval.

8. Security awareness and training

- All users must complete security awareness training on induction and at least annually thereafter.
- Training must include phishing awareness, safe remote working, password/MFA practices, data handling, and incident reporting.
- Targeted training must be provided for privileged users and system owners.

9. Compliance, monitoring and exceptions

- Compliance with this policy is mandatory. Breaches may result in disciplinary action and/or contractual remedies.
- Security controls may be monitored and audited (e.g., logging, device compliance reporting) for legitimate business and security purposes.
- Exceptions must be documented, risk-assessed, approved by the Information Security Lead and reviewed regularly with a defined end date.

10. Review

This policy will be reviewed at least annually and after significant changes (e.g., major incidents, new systems, significant supplier changes) to ensure it remains effective and aligned to business needs and the evolving threat landscape.

Policy owner	Damian Liptrot/Office Manager/IT Lead
Approved by	Dominic Liptrot/Managing Director
Effective date	01/01/2026
Review date	01/01/2027
Version	1.0