LOST ART
HISTORIC LANDSCAPE FURNISHING

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: RISK MANAGEMENT POLICY

1. Purpose and scope

This policy sets the minimum requirements for identifying, assessing, treating, monitoring and reporting risks that could affect the ability of Lost Art Limited to achieve its objectives.

- **In scope:** strategic, operational, financial, legal/regulatory, health & safety, information/cyber, project and reputational risks arising from UK activities.
- **Applies to:** all employees, agency staff, contractors and third parties acting on the organisation's behalf within all operations.
- **Interfaces:** this policy operates alongside specialist policies (e.g., information security, health & safety, safeguarding, business continuity, anti-fraud, procurement).
- **Out of scope:** personal risks unrelated to work; risks transferred fully to third parties by contract/insurance (though oversight and assurance remain in scope).

2. Policy statement and principles

The organisation will manage risk to protect and create value, support effective decision-making, and meet applicable UK legal and regulatory obligations. Our approach is consistent with recognised good practice (including ISO 31000:2018 principles) and, where applicable, UK corporate governance expectations for risk management and internal control.

Risk management will be:

- **Integrated** into governance, strategy, planning, delivery and change.
- **Structured and comprehensive** with consistent methods, records and reporting.
- **Customised** to our objectives, context, materiality and risk profile.
- **Inclusive** with clear accountability and engagement of relevant stakeholders.

- **Dynamic** and responsive to internal and external change.
- **Based on the best available information**, with assumptions documented.
- **Considering human and cultural factors**, including capability, workload and behaviour.
- **Continually improved** through lessons learned, assurance and review.

3. Governance, roles and responsibilities

Effective risk management requires clear ownership, oversight and independent assurance.

Role	Key responsibilities
Managing Director	Approve risk appetite and this policy; ensure an effective risk management and internal control framework; review principal risks at least annually; set the "tone from the top".
Managing Director and other management	Oversee the operation of the framework; review the corporate risk register; monitor control effectiveness and remediation; review assurance plans and significant incidents.
Managing Director	Implement this policy; ensure resources, competence and clear accountabilities; embed risk management into decision-making and performance management.
Office Management	Maintain the framework, tools and guidance; facilitate risk workshops; support risk owners; consolidate reporting; provide second-line oversight and challenge.
Risk owners (all managers)	Identify and assess risks in their area; maintain risk entries; ensure controls and actions are implemented; escalate material changes and incidents promptly.
Control owners	Design, operate, evidence and test controls (as assigned); remediate weaknesses.
Internal assessment by all staff	Where appropriate, provide independent assurance on the adequacy and effectiveness of governance, risk management and controls.
All employees and contractors	Manage risks within their work; follow required controls and procedures; report incidents, near misses and emerging risks.

4. Risk appetite and tolerances

Risk appetite is the amount and type of risk the organisation is willing to take in pursuit of its objectives. The Board (or equivalent) approves the risk appetite statement and key tolerances (quantitative and qualitative), and management operates within them.

4.1 Risk appetite statement

The organisation has a **cautious to balanced** risk appetite: we will take **measured and controlled** risks to deliver our strategy and improve performance, but we have a **low appetite** for risks that could cause serious harm to people, breach the law or regulation, undermine financial sustainability, or materially damage trust and reputation. Where we do accept higher levels of risk (e.g., during change and growth initiatives), it must be within approved tolerances, supported by robust controls and active monitoring.

Our appetite by risk area is typically:

- **Health & safety:** very low. We do not accept uncontrolled risks that could result in serious injury or ill health:
- **Legal/regulatory and ethics (including bribery, fraud, modern slavery):** very low. We aim for full compliance and prompt escalation of any suspected breach.
- **Information security and data protection:** low. We will accept only limited residual risk, proportionate to business need and protected by appropriate controls.
- **Financial:** low to balanced. We prioritise financial resilience and will take prudent risks where returns and downside exposures are understood and within tolerance.
- **Operational/service delivery:** balanced. We will accept reasonable operational risk to deliver services effectively, while maintaining continuity and quality standards.
- **Projects and change:** balanced to (occasionally) moderately high for approved strategic change, provided governance, stage gates and contingency plans are in place.
- **Reputational:** low. We will not knowingly take actions that could materially undermine stakeholder trust.
- Risk appetite and tolerances will be defined for key areas (e.g., health & safety, compliance, financial resilience, data protection, service performance, project delivery).
- Where tolerances are exceeded (or forecast to be exceeded), the risk owner (Managing Director) must escalate and agree corrective actions.
- **Minimum appetite (generally):** the organisation has low appetite (that could be more correctly expressed as NO APPETITE) for unlawful activity, fraud, bribery, serious health & safety harm, and non-compliance with statutory obligations.
- **Balanced appetite (example):** the organisation may accept measured operational or project risk to deliver strategic change, where impacts are understood and within agreed tolerances.

5. Risk management process

5.1 Establish context

Before assessing risk, the risk owner will define the objectives affected, the scope (process/project/site), stakeholders, dependencies, and the risk criteria (impact/likelihood scales and risk appetite/tolerances). Key assumptions and constraints must be recorded.

5.2 Identify risks

Risks will be described in a consistent format that distinguishes **cause**, **event** and **impact**. Identification methods may include workshops, incident/near-miss analysis, audits, horizon scanning, supplier reviews and project reviews.

5.3 Analyse and evaluate risks

Risks will be assessed for likelihood and impact, considering existing controls. Where practical, both **inherent risk** (before controls) and **residual risk** (after controls) will be recorded. The organisation will use defined scoring scales and thresholds to identify material/principal risks and required escalation.

5.4 Treat risks

Risk treatment will be proportionate to the risk and aligned to risk appetite. Treatment options include:

- **Avoid** (stop the activity or choose an alternative approach).
- **Reduce** (implement or improve preventive/detective/corrective controls).
- **Share/transfer** (e.g., insurance, outsourcing, contractual allocation), while retaining oversight of residual risk.
- **Accept** (where within appetite/tolerance and agreed by the appropriate authority).
- **Exploit/enhance** (for opportunity risks, where appropriate).

All material risks must have a documented treatment plan with clear actions, owners, target dates, required resources, dependencies and success measures. Overdue actions must be escalated.

5.5 Monitor, review and report

- Risk owners will review their risks at an agreed frequency (at least quarterly for material risks, or more frequently where conditions change).
- Key risk indicators (KRIs) and performance metrics will be used where appropriate to provide early warning.
- Risks will be re-assessed following significant change (e.g., new contracts, reorganisations, major incidents, regulatory change, supplier failure, material control failures).
- Management will provide regular reporting to the Audit & Risk Committee/Board, including principal risks, trend analysis, overdue actions and emerging risks.

5.6 Communicate and consult

Relevant internal and external stakeholders (including employees, clients/customers, suppliers, regulators and partners) will be engaged as appropriate to ensure risks are understood, assumptions are challenged and decisions are informed.

6. Risk categories

- **Strategic:** market change, funding, competitive position, partnerships, M&A, major transformation.
- **Operational:** service delivery failure, capacity, process breakdown, supply chain disruption, asset failure.
- **Financial:** liquidity, cash flow, credit, cost escalation, fraud, tax, pension obligations.
- **Legal and regulatory (UK):** compliance with applicable legislation and regulator requirements (e.g., Companies Act reporting duties as relevant; UK GDPR/Data Protection Act 2018; Bribery Act 2010; Modern Slavery Act 2015; health and safety law; employment law; sector-specific regulation).
- **Health, safety and environment:** workplace and site safety, occupational health, environmental impacts and permits.
- **Information and cyber:** confidentiality, integrity and availability of information; cyber attack; third-party IT risk; business email compromise; data loss.
- **Project and change:** scope, schedule and cost; design/quality; benefits realisation; change impacts and adoption.
- **Reputational:** customer harm, quality issues, complaints, media scrutiny, ethical conduct.

7. Risk registers, reporting and escalation

The organisation will maintain risk registers to support decision-making and oversight. A corporate risk register will capture principal/material risks, supported by local, programme/project and specialist registers where needed.

At a minimum, each risk entry will record:

- Risk title and description (cause–event–impact)
- Risk owner and (where applicable) control owner(s)
- Inherent and residual likelihood/impact ratings; overall risk rating
- Existing key controls (preventive/detective/corrective) and control effectiveness assessment
- Risk treatment actions, due dates, status and dependencies
- Key risk indicators (where used) and thresholds
- Assumptions, constraints, linked issues/incidents and interdependencies
- Last review date and next review date

Escalation: risks that exceed appetite/tolerance, have rapidly increasing trend, involve suspected unlawful activity, pose a credible risk of serious harm, or could materially impact objectives must be escalated immediately to the appropriate executive and, where required, to the Audit & Risk Committee/Board.

8. Internal controls and assurance

Controls are the measures in place to manage risk. The organisation will maintain an internal control framework covering (as applicable) financial, operational, reporting and compliance controls.

- **First line:** management owns and operates controls within day-to-day activities.
- **Second line:** risk/compliance functions provide oversight, challenge and support.
- **Third line:** internal audit provides independent assurance.
- Material controls will be identified for principal risks and reviewed at least annually (or more frequently where needed). Control deficiencies must have remediation plans, owners and target dates.

9. Incident, breach and near-miss management

- All incidents, near misses, control failures and significant complaints must be recorded and investigated proportionately to establish root causes and corrective actions.
- Potential regulatory reportable events (e.g., data breaches, notifiable safety incidents, financial misconduct) must be escalated immediately to the relevant responsible function for assessment and notification where required.
- Lessons learned will be incorporated into risk registers, procedures, training and control design.

10. Training, competence and culture

All staff must understand how risk management applies to their role. Risk owners and control owners must be competent to assess and manage risks, operate controls and maintain appropriate evidence. The organisation will promote an open, “speak up” culture where concerns can be raised without retaliation – **refer back to the Lost Art Limited Whistleblowing Policy**

11. Records management

Risk registers, assessments, treatment plans, control evidence and assurance reports are organisational records and must be stored securely

12. Review, compliance and exceptions

- This policy will be reviewed at least annually and after any significant organisational change, major incident or regulatory change (see Appendix B as all Lost Art Limited contracts/projects are bespoke).
- Compliance with this policy may be monitored through management review, audits, assurance activities and performance reporting.
- Any exceptions to this policy must be documented, time-bound and approved by the Document Owner in conjunction with the Managing Director and Contract Manager, with potential input from Sue Sharp in relation to financial risk.

Appendix A: Risk scoring

Likelihood (example)	Impact (example)
1 Rare: may occur only in exceptional circumstances	**1 Insignificant:** minimal disruption; no injury; negligible financial/reputational impact
2 Unlikely: could occur at some time	**2 Minor:** limited disruption; minor injury/first aid; small financial impact
3 Possible: might occur at some time	**3 Moderate:** measurable disruption; reportable incident possible; moderate financial impact
4 Likely: will probably occur in most circumstances	**4 Major:** significant disruption; serious harm possible; major financial/reputational impact
5 Almost certain: expected to occur in most circumstances	**5 Severe:** critical disruption; severe harm; very large financial/reputational impact

Appendix B: Escalation and reporting thresholds (placeholder)

Thresholds for escalation are to be allocated on a contract by contract basis other than those that are ongoing throughout a calendar

Policy owner	Damian Liptrot/Office Manager
Approved by	Dominic Liptrot/Managing Director
Effective date	01/01/2026

Review date	01/01/2027
Version	26/1