OCLAS
OPERATIONAL PERFORMANCE IN ENERGY AND INFRASTRUCTURE

Data Protection, Privacy and Information Security Policy

UK GDPR controls, security baseline and incident response

Document reference	OCL-GOV-002
Owner	Sheyi N. Lisk-Carew, Founder and Principal
Effective date	1 September 2026
Review date	1 September 2027

Purpose: To protect personal and confidential information through proportionate governance, secure technology, controlled access and auditable handling throughout its lifecycle.

Scope and accountability

This policy applies to Sheyi N. Lisk-Carew, trading as Oclas, any authorised associate or subcontractor, and all Oclas systems, devices, records and client information. The Founder and Principal is accountable for privacy governance and acts as the contact for data-subject and security enquiries. Specialist legal or security advice is obtained where risk or contract terms require it.

Data-protection principles

- Process personal data lawfully, fairly and transparently for defined purposes.
- Collect only what is necessary; keep it accurate; retain it only for an evidenced legal, contractual or business need.
- Protect confidentiality, integrity and availability and be able to demonstrate compliance.
- Use privacy information and, where consent is relied upon, obtain active, informed, specific and auditable consent that can be withdrawn.

Information governance

- Maintain a data and processing register covering purpose, lawful basis, categories, recipients, locations, retention, security measures and international transfers.
- Classify information as Public, Internal, Confidential or Restricted and apply handling controls proportionate to sensitivity.
- Complete a data-protection impact assessment before high-risk processing, systematic monitoring or use of novel technology involving personal data.
- Use written data-processing terms and due diligence for suppliers that process personal data on Oclas's behalf.

Technical and organisational controls

- Multi-factor authentication for business-critical cloud services and privileged access; unique accounts; least privilege; and timely removal of access.
- Full-disk encryption on supported endpoints; encrypted transport using current TLS; and encryption at rest for cloud services handling Confidential or Restricted information where supported and contractually appropriate.
- Supported operating systems, security updates, malware protection, screen locking, secure configuration and prohibited use of unapproved storage or transfer services.
- Version-controlled working files, tested backup or recoverability arrangements for critical records, and documented continuity procedures for loss of a device, service or premises.
- Secure deletion or verified return at the end of the retention period, engagement or supplier relationship.

Data-subject rights and records

Requests for privacy information, access, rectification, erasure, restriction, objection or portability are logged and handled without undue delay. Identity is verified proportionately. Requests and complaints should be sent to onliskcarew@oclasgroup.com. Oclas maintains an auditable record of the request, decision, action and response.

International transfers

Personal data is not transferred outside the UK unless the transfer is necessary and a valid safeguard is documented, such as UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to approved standard contractual clauses. Transfer risk is assessed before use.

Incident response

1. Contain the incident, protect people and systems, and preserve evidence.
2. Record what happened, the data and people affected, likely consequences and mitigation.
3. Assess legal, contractual and client-notification duties immediately, including the UK GDPR 72-hour regulatory timescale where applicable.
4. Notify affected clients, individuals, the ICO or other authorities when required, with accurate and controlled communications.
5. Recover services, test integrity, close corrective actions and record lessons learned.

Testing and assurance

Access, supplier, backup, retention and incident controls are reviewed at least annually and after material change or incident. Buyer-specific security schedules are assessed before contract start and incorporated into the delivery plan. Gaps are recorded with an owner and due date.

Approval and control

Compliance with this policy is a condition of access to Oclas or client information. Deliberate or negligent breaches may lead to access withdrawal, contract action and regulatory notification where required.

Approved by: Sheyi N. Lisk-Carew, Founder and Principal | **Version:** 1.0
Legal bidder: Sheyi N. Lisk-Carew, trading as Oclas | **Contact:** onliskcarew@oclasgroup.com