Nexus 360

Records Management Policy

Staff Group to whom it applies:	All employees, contractors, consultants and third parties acting on behalf of Nexus 360.
How to access the document:	Nexus 360 computer systems.
Issue date:	June 2026
Version:	1.0
Date of next review:	June 2027
Developed by:	Danielle Cocksedge – Data Protection and Governance Manager – ARC Management and Consultancy Services
Approved by:	Mark Shevill – Director
Amendments/Updates: **Version 1.0**	New policy created for Business need.

1. Policy Statement

Information is a vital organisational asset of Nexus 360 and is essential to the effective delivery of services, regulatory compliance, business continuity, client relationship management, digital engagement services and operational decision-making.

Nexus 360 relies upon accurate, reliable and accessible information to support the delivery of CRM solutions, automation services, digital business card platforms, marketing technologies and consultancy services.

Effective records management ensures that information is:

- Accurate and reliable
  • Secure and confidential
  • Accessible when required
  • Properly retained and disposed of
  • Managed in accordance with legal, regulatory and contractual obligations

Records maintained by Nexus 360 form part of the organisation's corporate memory and provide evidence of:

- Decisions made
  • Actions taken
  • Services delivered
  • Client interactions
  • Communications and agreements
  • Compliance with legal and regulatory requirements

Effective records management supports:

- Protection of organisational interests and assets
  • Protection of the rights of clients, employees, suppliers and stakeholders
  • Transparency and accountability
  • Business continuity and operational resilience
  • Compliance with information governance requirements
  • Efficient use of physical and electronic storage systems
  • Reduction of legal, regulatory and information security risks

This policy should be read alongside the Nexus 360 Data Protection and UK GDPR Policy, Information Security Policy, Privacy Notice, Retention Schedule, Incident Management Procedures and other supporting governance documentation.

2. Purpose

The purpose of this policy is to establish effective governance arrangements and responsibilities for the creation, management, storage, retention, access, archiving and disposal of records across Nexus 360.

The objectives of this policy are to ensure records:

- Support informed and effective decision-making
  • Provide evidence of business activities, decisions and actions
  • Support business continuity and operational efficiency
  • Demonstrate accountability and transparency
  • Support investigations, complaints handling and legal proceedings where necessary
  • Protect the rights, assets and interests of Nexus 360 and its stakeholders
  • Support compliance with legal, regulatory, contractual and operational obligations
  • Are managed securely throughout their lifecycle

3. Scope

This policy applies to:

- Directors
  • Employees
  • Contractors
  • Consultants
  • Temporary staff
  • Agency workers
  • Third-party suppliers
  • Sub-processors
  • Anyone creating, managing or handling records on behalf of Nexus 360

This policy applies to all records created, received, processed, stored or managed by Nexus 360 in any format, including but not limited to:

Corporate and Administrative Records

- Policies and procedures
  • Governance documentation
  • Contracts and agreements
  • Board and management records
  • Meeting minutes and action logs
  • Business continuity documentation
  • Audit records

Employee Records

- Recruitment records
  - Personnel files
  - Training records
  - Performance management records
  - Payroll information
  - Occupational health records where applicable

Client and Service Records

- CRM records
  - Client account information
  - Service delivery records
  - Support requests and tickets
  - Consultancy documentation
  - Project records
  - Client communications

Marketing and Digital Engagement Records

- Marketing campaign records
  - Consent records
  - Preference management records
  - Digital business card interactions
  - Website enquiries
  - Lead management records

Financial Records

- Accounting records
  - Invoices
  - Purchase records
  - Tax documentation
  - Banking records

Electronic and Digital Records

- Emails
  - Databases
  - Electronic documents
  - Cloud storage records
  - Website content
  - CRM platforms
  - Automation systems
  - Mobile device records
  - Audio and video recordings
  - Metadata generated by systems

Physical Records

- Paper documents
  - Printed correspondence
  - Archived hard-copy files
  - Photographs and images

This list is not exhaustive.

4. Roles and Responsibilities

4.1 Director

The Director retains overall accountability for records management and information governance within Nexus 360.

Responsibilities include:

- Ensuring effective governance arrangements are in place
  - Supporting compliance with legal and regulatory obligations
  - Ensuring adequate resources are available
  - Promoting a culture of good information governance and accountability
  - Monitoring organisational risks associated with records management

4.2 Outsourced Data Protection Officer (DPO)

The Outsourced Data Protection Officer provides independent advice and oversight regarding records management and information governance.

Responsibilities include:

- Advising on records management and data protection compliance
  - Monitoring compliance with information governance obligations
  - Supporting staff awareness and training
  - Advising on retention, disposal and information sharing arrangements
  - Supporting Subject Access Requests and information rights requests
  - Advising on records relating to personal information and privacy obligations

4.3 Employees, Contractors and Authorised Users

All personnel are responsible for:

- Creating and maintaining accurate records relating to their work activities
  - Managing records in accordance with this policy and associated procedures
  - Maintaining confidentiality and security of records
  - Reporting any loss, unauthorised disclosure or misuse of records
  - Ensuring records are retained and disposed of appropriately
  - Following all information security and data protection requirements

Personnel must recognise that records containing personal information are subject to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Confidentiality obligations
- Nexus 360 governance policies and procedures

5. Legal and Regulatory Compliance

This policy supports compliance with:

- UK General Data Protection Regulation (UK GDPR)
  - Data Protection Act 2018
  - Privacy and Electronic Communications Regulations (PECR)
  - Freedom of Information Act principles where applicable
  - Human Rights Act 1998
  - Computer Misuse Act 1990
  - Copyright, Designs and Patents Act 1988
  - Limitation Act 1980
  - Electronic Communications Regulations
  - Information Commissioner's Office (ICO) guidance and standards
  - Applicable contractual and industry obligations

Nexus 360 shall ensure records are managed lawfully, fairly, transparently, securely and in accordance with recognised information governance principles.

6. Records Management Principles

Nexus 360 is committed to ensuring records are managed in accordance with the following principles.

6.1 Quality and Integrity

Records shall be:

- Accurate
  - Complete
  - Reliable
  - Authentic
  - Up to date where appropriate

Records must provide sufficient context to demonstrate how decisions and actions were reached.

6.2 Accessibility

Records and information shall be:

- Accessible to authorised individuals when required
  - Organised and indexed appropriately

- Retrievable within reasonable timescales
- Maintained in formats that remain usable and readable
- Subject to version control where appropriate

6.3 Security and Confidentiality

Appropriate technical and organisational measures shall be implemented to protect records against:

- Unauthorised access
- Accidental loss
- Alteration or destruction
- Misuse or disclosure

Security measures may include:

- Access controls and permissions
- Password protection
- Multi-factor authentication
- Encryption technologies
- Secure cloud storage
- Cyber security controls
- Backup and recovery arrangements
- Confidential waste disposal procedures

6.4 Retention and Disposal

Records shall only be retained for as long as necessary to fulfil legal, regulatory, contractual, operational or business requirements.

Unless a longer retention period applies:

- Personal information will normally be actively retained for three years
- Information may then be securely archived for up to six additional years where required for legal, operational, contractual, financial, insurance or audit purposes
- Records relating to ongoing disputes, investigations, complaints, legal proceedings or regulatory matters may be retained for longer where justified

At the end of the retention period, records shall be securely disposed of through:

- Confidential shredding of paper records
- Secure deletion of electronic records
- Permanent destruction of storage media where appropriate
- Anonymisation where appropriate

Retention and disposal activities shall comply with organisational retention schedules and applicable legislation.

6.5 Training and Awareness

All personnel shall receive appropriate records management and information governance training through:

- Induction processes
  • Compliance training
  • Policy awareness activities
  • Refresher training where required

6.6 Monitoring and Continuous Improvement

Records management arrangements shall be regularly monitored and reviewed to ensure compliance, effectiveness and continual improvement.

Monitoring activities may include:

- Internal audits
  • Compliance reviews
  • Spot checks
  • Incident monitoring
  • Corrective action planning

7. Information Rights and Access Requests

Individuals have the right to request access to personal information held about them under UK data protection legislation.

Requests may relate to:

- Employee records
  • Client records
  • Marketing records
  • CRM information
  • Electronic records
  • Paper records

Requests may be submitted using the contact details contained within the Nexus 360 Privacy Notice available at:

https://nexus360.digital/

Nexus 360 shall process requests in accordance with:

- UK GDPR
  • Data Protection Act 2018
  • ICO guidance and statutory response times

Identity verification may be required before information is disclosed.

Information sharing shall only take place where:

- A lawful basis exists
  • Consent has been obtained where required
  • Sharing is necessary for legal, contractual, safeguarding, regulatory or operational purposes
  • Appropriate safeguards are in place

8. Data Breaches and Incident Reporting

Any actual or suspected:

- Personal data breach
  • Loss of records
  • Unauthorised disclosure
  • Security incident involving information or records
  • Cyber security incident

must be reported immediately in accordance with Nexus 360 Incident Management and Data Protection procedures.

Incidents shall be investigated and reported to relevant authorities, including the Information Commissioner's Office where legally required.

9. Non-Compliance

Failure to comply with this policy may result in:

- Corrective action
  • Removal of access to systems or records
  • Disciplinary action
  • Termination of contracts or supplier arrangements
  • Legal or regulatory action where appropriate

10. Related Policies and Documents

This policy should be read alongside:

- Data Protection and UK GDPR Policy
  • Information Security Policy
  • Privacy Notice
  • Data Retention Schedule
  • Incident Policy
  • Business Continuity Plan
  • Supplier Management Procedures
  • Confidentiality Agreements