**Nexus 360**

**Data Protection and UK GDPR 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:**<br>**Version 1.0** | New policy created for Business need. |

## 1. Policy Statement

Nexus 360 is committed to protecting the privacy, confidentiality, integrity and availability of personal information and ensuring compliance with all applicable data protection legislation.

The organisation recognises that personal information is a valuable business asset and that individuals have a fundamental right to expect their information to be handled responsibly, securely and transparently.

This policy establishes the framework through which Nexus 360 fulfils its obligations under:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Human Rights Act 1998
- Computer Misuse Act 1990
- Applicable contractual, regulatory and industry requirements

Nexus 360 is committed to demonstrating accountability and embedding privacy, information governance and data protection into all business processes, systems and services.

This policy should be read in conjunction with the Nexus 360 Privacy Notice, Information Security Policy, Data Processing Agreements, Data Retention Schedule and other supporting governance documentation.

The Nexus 360 Privacy Notice explains how personal information is collected, used, stored, shared, transferred and protected and is available:

- Via the Nexus 360 website - https://nexus360.digital/
- Upon request from Nexus 360;

All personnel must ensure that their processing activities remain consistent with the commitments made within the Privacy Notice.

## 2. Purpose

The purpose of this policy is to:

- Protect personal information processed by Nexus 360;
- Define responsibilities for data protection compliance;
- Ensure lawful, fair and transparent processing;
- Reduce risks associated with personal data breaches;

- Protect the rights and freedoms of individuals;
- Support clients who entrust Nexus 360 with personal information;
- Establish a culture of privacy, security and accountability throughout the organisation;
- Demonstrate compliance with applicable data protection legislation and recognised good practice.

## 3. Scope

This policy applies to:

- Directors;
- Employees;
- Contractors;
- Consultants;
- Temporary staff;
- Agency workers;
- Third-party suppliers;
- Sub-processors;
- Anyone processing information on behalf of Nexus 360.

The policy applies to all personal information processed by Nexus 360 regardless of format, including:

- Electronic records;
- Cloud-based systems;
- CRM platforms;
- Client portals;
- Digital business card solutions;
- Automation platforms;
- Marketing systems;
- Email communications;
- Mobile devices;
- Physical records;
- Business applications;
- Website and online services.

This policy applies whether Nexus 360 is acting as a Data Controller or a Data Processor on behalf of clients.

## 4. Data Protection Principles

Nexus 360 shall ensure that all personal information is processed in accordance with the principles set out within UK GDPR.

**Lawfulness, Fairness and Transparency**

Personal information shall only be processed where an appropriate lawful basis exists and individuals are provided with clear information regarding how their information is used.

**Purpose Limitation**

Personal information shall only be collected for specified, explicit and legitimate purposes and shall not be processed in a manner incompatible with those purposes.

**Data Minimisation**

Only information that is relevant, adequate and necessary for the intended purpose shall be collected and processed.

**Accuracy**

Reasonable steps shall be taken to ensure that personal information remains accurate and up to date.

**Storage Limitation**

Personal information shall not be retained for longer than necessary and shall be managed in accordance with the organisation's retention requirements.

**Integrity and Confidentiality**

Appropriate technical and organisational measures shall be implemented to protect personal information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

**Accountability**

Nexus 360 shall maintain appropriate records, policies, procedures and controls to demonstrate compliance with data protection legislation.

## 5. Governance and Accountability

The Director retains overall accountability for data protection compliance within Nexus 360.

To demonstrate accountability, Nexus 360 shall maintain appropriate governance arrangements including:

- Privacy Notices;
- Data Processing Agreements;
- Supplier and Sub-Processor Records;
- Information Security Procedures;
- Data Breach Registers;
- Data Subject Request Logs;

- Training Records;
- Asset Registers;
- Information Asset Inventories;
- Confidentiality Agreements;
- Data Retention Schedules;
- Risk Assessments and Privacy Impact Assessments where appropriate.

Data protection and information security considerations shall be incorporated into:

- Business planning;
- Service development;
- Software implementation;
- CRM deployments;
- Automation solutions;
- Marketing activities;
- Supplier selection and management.

Nexus 360 recognises Privacy by Design and Default as a core principle and seeks to embed privacy and security controls into all systems and services from the outset.

## 6. Roles and Responsibilities

**Director**

The Director is responsible for:

- Strategic oversight of data protection compliance;
- Allocation of appropriate resources;
- Monitoring organisational compliance;
- Managing information governance risks;
- Approving policies and procedures;
- Ensuring data protection remains a business priority.

**Outsourced Data Protection Officer (DPO)**

Nexus 360 has appointed an independent outsourced Data Protection Officer to provide specialist advice, support and oversight regarding compliance with data protection legislation.

The Outsourced DPO acts independently and supports Nexus 360 by:

- Advising on UK GDPR, Data Protection Act 2018 and PECR compliance;
- Monitoring the effectiveness of data protection controls and governance arrangements;

- Reviewing policies, procedures and privacy documentation;
- Supporting the management of Subject Access Requests and individual rights requests;
- Advising on personal data breaches and regulatory reporting requirements;
- Supporting Privacy Impact Assessments and Privacy by Design activities;
- Reviewing supplier and sub-processor compliance arrangements;
- Providing data protection guidance and awareness support;
- Acting as an escalation point for complex data protection issues;
- Liaising with the Information Commissioner's Office (ICO) where required.

The contact details for the Outsourced DPO are maintained within the Nexus 360 Privacy Notice.

**Employees and Contractors**

All employees, contractors and authorised users of Nexus 360 systems must:

- Follow this policy and all associated procedures;
- Protect personal information at all times;
- Maintain confidentiality;
- Report actual or suspected data breaches immediately;
- Complete mandatory training and awareness activities;
- Use business systems responsibly and securely;
- Comply with access control requirements and security measures.

Failure to comply with this policy may result in disciplinary action, removal of access rights, termination of contracts and, where appropriate, legal action.

## 7. Lawful Processing

Personal information shall only be processed where an appropriate lawful basis exists.

These may include:

- Contract
- Legal Obligation
- Legitimate Interests
- Consent
- Vital Interests
- Public Task (where applicable)

Staff must ensure that:

- Individuals receive privacy information
- Processing is documented

- Lawful bases are identified
- Consent is obtained where required

## 8. Privacy by Design and Default

Nexus 360 shall incorporate privacy considerations into:

- New services
- CRM deployments
- Automation systems
- Marketing platforms
- Website development
- Software integrations
- Business processes

Where appropriate, privacy risks shall be assessed before implementation.

## 9. Information Security

Nexus 360 shall maintain appropriate technical and organisational measures including:

Access Control

- Unique user accounts
- Strong passwords
- Multi-factor authentication
- Least privilege access
- Regular access reviews

Technical Controls

- Endpoint protection
- Encryption technologies
- Secure backups
- Firewall protection
- Vulnerability management
- Patch management
- Malware protection
- Secure configuration standards

Physical Security

- Secure premises
- Device protection
- Visitor management controls
- Confidential waste disposal

Monitoring

- Audit logs
- Security monitoring
- Incident detection
- Access monitoring

## 10. CRM, Automation and Platform Management

Given Nexus 360's provision of CRM, automation and digital engagement solutions, additional controls apply.

The organisation shall:

- Restrict access to authorised personnel
- Maintain logical separation of client environments where feasible
- Monitor administrative access
- Record significant system activity
- Review permissions regularly
- Secure onboarding and offboarding processes
- Maintain backup and recovery arrangements

Where client data is hosted or processed within Nexus 360-managed platforms, security controls shall be proportionate to identified risks.

## 11. Data Controller and Data Processor Responsibilities

Nexus 360 may act as either:

### Data Controller

When processing information relating to:

- Employees
- Clients
- Suppliers
- Prospective customers
- Marketing contacts

### Data Processor

When processing information on behalf of clients through:

- CRM systems
- Client portals
- Marketing platforms
- Digital business card solutions
- Automation systems
- Hosted business applications

When acting as a processor, Nexus 360 shall:

- Process information only under instruction
- Maintain confidentiality
- Implement appropriate security measures
- Assist controllers where required
- Report breaches promptly

## 12. Supplier and Sub-Processor Management

Nexus 360 shall take reasonable steps to ensure that suppliers handling personal information provide appropriate security and privacy protections.

Supplier assessments may consider:

- Security certifications
- Data protection commitments
- Privacy practices
- Incident management arrangements
- International transfer considerations

Written agreements shall be maintained where required.

## 13. Marketing Compliance

Marketing activities must comply with UK GDPR and PECR.

Nexus 360 shall:

- Obtain consent where required
- Maintain suppression lists
- Record marketing preferences
- Enable easy opt-out options
- Respect opt-out requests
- Monitor marketing compliance

Marketing communications shall be clear, transparent and lawful.

## 14. Artificial Intelligence and Automation

Where AI tools or automation technologies are utilised:

- Human oversight shall be maintained where appropriate
- Outputs shall be reviewed before significant business decisions are made
- Personal information shall only be processed in accordance with applicable legislation
- Risks associated with automated processing shall be assessed

Clients remain responsible for configurations they implement within their own environments or systems.

## 15. Data Subject Rights

Nexus 360 shall support the exercise of individual rights including:

- Access
- Rectification
- Erasure
- Restriction
- Objection
- Portability
- Withdrawal of consent

All requests must be referred immediately to the Data Protection Officer.

Requests shall be handled within statutory timescales.

## 16. Personal Data Breaches

All actual, suspected or potential personal data breaches must be reported immediately.

Nexus 360 shall:

- Investigate incidents
- Assess risk
- Contain breaches
- Document findings
- Implement corrective actions
- Notify regulators where required
- Notify affected individuals where required

A breach register shall be maintained.

## 17. Data Retention and Disposal

Personal information shall:

- Be retained only for legitimate business purposes
- Be reviewed regularly
- Be securely deleted when no longer required
- Be destroyed using appropriate methods

Retention periods shall be defined within organisational retention schedules.

## 18. Training and Awareness

All personnel shall receive appropriate training covering:

- Data protection principles
- Security awareness
- Phishing awareness

- Incident reporting
- Confidentiality obligations
- Acceptable use requirements

Training records shall be maintained.

## 19. Monitoring, Audit and Compliance

Compliance may be monitored through:

- Internal reviews
- Access audits
- Incident reviews
- Supplier reviews
- Security assessments
- Management oversight

Findings shall be addressed through corrective actions where appropriate.

## 20. Policy Review

This policy shall be reviewed:

- Annually
- Following legislative changes
- Following significant organisational changes
- Following major incidents
- Where new processing activities create additional risks

All amendments shall be formally approved and version controlled.