



Nexus 360

BEYOND AMBITION → STRUCTURED GROWTH

Nexus 360

Confidentiality 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:	July 2026
Version:	1.0
Date of next review:	July 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

Nexus 360 is committed to protecting the confidentiality, integrity and security of all information entrusted to the organisation.

The organisation recognises that confidential information is essential to maintaining the trust of clients, employees, contractors, suppliers and business partners. All confidential information must be handled appropriately and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable legislation.

Every individual working for or on behalf of Nexus 360 has a responsibility to protect confidential information from unauthorised access, disclosure, alteration, loss or misuse.

Failure to comply with this policy may result in disciplinary action and, where appropriate, legal or contractual action.

2. Purpose

The purpose of this policy is to ensure that confidential information is handled consistently, securely and lawfully throughout Nexus 360.

The objectives are to:

- Protect confidential business and personal information.
- Ensure compliance with UK GDPR and the Data Protection Act 2018.
- Prevent unauthorised disclosure of information.
- Promote good information governance practices.
- Protect the rights and privacy of clients, employees and third parties.
- Support the secure sharing of information where there is a lawful basis to do so.

3. Scope

This policy applies to:

- Directors
- Employees
- Contractors
- Consultants

- Temporary staff
- Agency workers
- Third-party suppliers
- Anyone acting on behalf of Nexus 360

This policy applies to all confidential information held or processed by Nexus 360 in electronic, paper, verbal or any other format.

4. Definition of Confidential Information

Confidential information includes any information that is not publicly available and which has been obtained through employment or engagement with Nexus 360.

This includes, but is not limited to:

- Personal data relating to clients, employees or contractors.
- Financial information.
- Commercially sensitive information.
- Business plans and strategies.
- Contracts and legal documentation.
- Payroll and employment records.
- Client records and correspondence.
- Passwords, access credentials and security information.
- Information received from third parties under a duty of confidence.

Confidential information may exist in paper files, electronic systems, emails, databases, photographs, recordings or verbal communications.

5. Principles of Confidentiality

Nexus 360 will ensure that confidential information is:

- Accessed only by authorised individuals.
- Used only for legitimate business purposes.
- Shared only where there is a lawful basis or business need.
- Stored securely using appropriate technical and organisational measures.
- Protected against accidental or unlawful disclosure.
- Retained only for as long as necessary.
- Securely disposed of when no longer required.

All Personnel are expected to maintain confidentiality both during and after their employment or engagement with Nexus 360.

6. Responsibilities

All staff are responsible for maintaining confidentiality at all times.

Personnel must:

- Access confidential information only where authorised.
- Keep confidential information secure.
- Ensure confidential conversations cannot be overheard by unauthorised persons.
- Lock computers when unattended.
- Keep passwords secure and confidential.
- Verify recipients before sending emails or documents.
- Store paper records securely.
- Dispose of confidential waste using approved disposal methods.
- Immediately report any actual or suspected confidentiality breach.

Directors and Managers are responsible for ensuring that staff understand and comply with this policy and ensuring suitable governance arrangements are maintained.

7. Handling Confidential Information

Confidential information must be handled securely at all times.

Staff must:

- Only access information necessary to perform their duties.
- Avoid discussing confidential information in public places.
- Ensure documents are not left unattended.
- Use secure methods when transferring confidential information electronically.
- Ensure portable devices containing confidential information are appropriately protected and backed up.
- Follow organisational procedures for the storage, transfer and disposal of confidential information.

Confidential information must never be disclosed for personal gain or any unauthorised purpose.

8. Sharing Confidential Information

Confidential information will only be shared where:

- The individual has provided valid consent.
- There is a lawful basis under UK GDPR.
- Disclosure is required by law.
- Disclosure is necessary to protect an individual's vital interests.
- Disclosure is permitted under another applicable legal obligation.

Before sharing confidential information, staff must ensure:

- The recipient is authorised to receive the information.
- Only the minimum necessary information is disclosed.
- Appropriate security measures are used during transmission.

Where uncertainty exists, advice should be sought from a Director or the outsourced Data Protection Officer before disclosure.

9. Information Security

Nexus 360 will implement appropriate technical and organisational measures to protect confidential information.

These include:

- Password-protected systems.
- Role-based access controls.
- Secure storage of paper records.
- Encryption where appropriate.
- Secure disposal of confidential information.
- Physical security of offices and equipment.
- Regular review of access permissions.

Staff must immediately report lost devices, unauthorised access or suspected security incidents.

10. Breaches of Confidentiality

Any actual or suspected breach of confidentiality must be reported immediately to the Director.

Examples include:

- Loss of confidential documents.
- Sending information to the wrong recipient.
- Unauthorised access to records.

- Discussing confidential information with unauthorised individuals.
- Loss or theft of devices containing confidential information.

Nexus 360 will investigate all reported breaches and take appropriate corrective action.

Where a breach involves personal data, the organisation will assess whether notification to the Information Commissioner's Office (ICO) or affected individuals is required with the assistance of the outsourced Data Protection Officer.

11. Training

Nexus 360 will ensure that all Personnel receive appropriate confidentiality and data protection training.

Training will include:

- Induction training for new staff.
- Refresher training at regular intervals.
- Updates following legislative or organisational changes.

Personnel are responsible for maintaining their understanding of confidentiality requirements.

12. Monitoring and Compliance

Compliance with this policy will be monitored through:

- Internal audits.
- Information governance reviews.
- Incident reporting.
- Management oversight.
- Policy reviews.

Failure to comply with this policy may result in disciplinary action, termination of contracts or legal proceedings where appropriate.

13. Data Protection Officer (DPO) Involvement

The Outsourced Data Protection Officer (DPO) will provide advice and support in relation to:

- Confidentiality obligations.
- Complex information sharing decisions.
- Personal data breaches.
- Data protection compliance.
- Information governance matters.

- Investigations involving confidential information.

The DPO will provide guidance to ensure Nexus 360 complies with UK GDPR and associated legislation.

14. Record Keeping

Nexus 360 will maintain appropriate records relating to:

- Confidentiality incidents.
- Data breaches.
- Investigations.
- Staff training.
- Policy reviews.
- Corrective actions taken.

Records will be stored securely and retained in accordance with the organisation's Records Management Policy.

[LOGO]

Staff Confidentiality Agreement

Declaration

I acknowledge that during the course of my employment or engagement with Nexus 360, I may have access to confidential information relating to the organisation, its clients, employees, contractors, suppliers and business operations.

I understand that all confidential information, regardless of its format, must be protected and only accessed, used or disclosed where authorised and necessary for the performance of my duties.

I confirm that I have read and understood the Nexus 360 Confidentiality Policy and agree to comply with its requirements at all times.

I understand that my duty of confidentiality continues after my employment or engagement with Nexus 360 has ended.

I understand that any breach of confidentiality may result in disciplinary action, up to and including dismissal, termination of contract, legal proceedings and/or referral to the appropriate regulatory authorities where applicable.

I agree to:

- Protect all confidential and personal information entrusted to me.
- Access confidential information only where authorised and required for my role.
- Not disclose confidential information to any unauthorised person.
- Follow all Nexus 360 policies relating to confidentiality, information security and data protection.
- Keep passwords and system access credentials secure.
- Report any actual or suspected confidentiality breach immediately to a Director.
- Return all confidential information and organisational property upon leaving Nexus 360.

- Continue to maintain confidentiality after my employment or engagement has ended.

Employee Name: _____

Job Title: _____

Signature: _____

Date: _____

Appendix 2

[LOGO]

Third Party Confidentiality Agreement

Declaration

I acknowledge that whilst providing services to Nexus 360, I may have access to confidential information relating to the organisation, its clients, employees, contractors, suppliers and business operations.

I understand that this information remains the property of Nexus 360 and must only be used for the purposes of fulfilling my contractual obligations.

I confirm that I have read and understood the Nexus 360 Confidentiality Policy and agree to comply with its requirements throughout the duration of my engagement.

I understand that any breach of confidentiality may result in termination of my contract, legal action and notification to my employer or contracting organisation where appropriate.

I agree to:

- Maintain the confidentiality of all information obtained whilst working for or on behalf of Nexus 360.
- Use confidential information only for authorised business purposes.
- Prevent unauthorised access to confidential information.
- Store confidential information securely.
- Not copy, remove or disclose confidential information unless authorised.
- Immediately report any actual or suspected confidentiality or information security breach.
- Return or securely destroy all confidential information at the end of my contract, in accordance with Nexus 360's instructions.
- Continue to maintain confidentiality after my contract has ended.

Name: _____

Company: _____

Position: _____

Signature: _____

Date: _____

Nexus 360 Director: _____

Signature: _____

Date: _____