

Confidential Information Policy

Introduction and Commitment

Capital Sky Ltd is committed to ensuring that all confidential, sensitive, and commercially valuable information is properly protected. In the course of our work, employees, contractors, and other authorised personnel may have access to personal data, commercial information, and internal business records relating to clients, subcontractors, suppliers, and the company itself.

We recognise that the protection of this information is essential not only to comply with legal obligations but also to maintain trust, safeguard our reputation, and protect the commercial integrity of the business.

This policy applies to all employees, directors, contractors, agency workers, consultants, and any other individuals who may have access to Capital Sky information systems or confidential data. It must be read in conjunction with the Capital Sky Cyber Security Policy, Data Protection Policy, Data Breach Response Procedure, and Digital Information Handling Standard.

Purpose of This Policy

The purpose of this policy is to ensure that confidential information is handled securely, lawfully, and consistently across the organisation.

Confidential information must be protected in order to comply with legal and regulatory requirements, including the [UK GDPR](#) and the [Data Protection Act 2018](#), and to safeguard Capital Sky's commercial position, intellectual property, and operational security.

What We Consider Confidential Information

Confidential information includes any information that is not publicly available and which could cause harm, financial loss, reputational damage, or competitive disadvantage if disclosed without authorisation.

This includes, but is not limited to, financial information, client data, supplier and subcontractor details, pricing structures, commercial strategies, tender information, internal procedures, project documentation, and any information formally marked as confidential.

It also includes personal data relating to employees, clients, and third parties, as well as digital information stored on company systems, cloud platforms, mobile devices, or project management tools.

Handling of Confidential Information

All confidential information must be handled with care and only accessed by individuals who have a legitimate business need to do so.

Employees must ensure that confidential information is stored securely at all times, whether in physical or electronic format. Paper documents must be kept secure when not in use, and electronic information must only be accessed through Capital Sky-approved systems and devices.

Confidential information must only be discussed or shared with colleagues when it is necessary for business purposes and where the recipient is authorised to receive it. Care must be taken to ensure that sensitive discussions are not overheard or accessed by unauthorised individuals.

When confidential information is no longer required, it must be securely destroyed or permanently deleted in accordance with company procedures.

Restrictions on Use and Disclosure

Employees and authorised personnel must not use confidential information for personal gain, commercial advantage, or any purpose outside their employment or engagement with Capital Sky. Confidential information must not be disclosed to any external party unless there is a lawful business reason and appropriate authorisation has been obtained. This includes clients, family members, competitors, and any other third party.

Confidential information must never be stored on personal devices, personal email accounts, or unapproved cloud platforms. It must also not be transmitted using unsecured communication methods such as personal messaging applications or unencrypted file-sharing services.

Upon termination of employment or engagement, all confidential information must be returned or permanently deleted, and access to all Capital Sky systems will be revoked.

Security Measures and Controls

Capital Sky Ltd applies appropriate technical and organisational measures to protect confidential information from loss, misuse, unauthorised access, or disclosure.

These measures include secure storage of documents, encryption of sensitive data, controlled access based on job roles, multi-factor authentication, secure backup systems, firewalls, endpoint protection, and continuous monitoring of IT systems.

Access to confidential information is granted strictly on a need-to-know basis. All users are required to comply with company cyber security requirements, including password standards, system usage rules, and approved software controls.

All relevant personnel are required to complete cyber security and data protection training and must comply with the Capital Sky Cyber Security Policy at all times.

Third Parties and Subcontractors

Any subcontractor, consultant, agency worker, or third party engaged by Capital Sky must comply with the same confidentiality and security standards as employees.

Where appropriate, confidentiality agreements or contractual clauses will be used to ensure obligations are clearly defined and enforceable.

Failure to comply with these requirements may result in termination of the engagement and, where necessary, legal action.

Exceptions to Disclosure

Confidential information may only be disclosed where there is a lawful basis to do so, such as when required by law, regulation, court order, or regulatory authority, or when necessary for legitimate business purposes including audits, due diligence, or contractual obligations.

In all cases, disclosure must be limited to the minimum necessary information, must be properly authorised where required, and must be fully documented.

Breach of Confidentiality

Any suspected or actual breach of confidentiality must be reported immediately in line with the Capital Sky Data Breach Response Procedure.

Breaches of this policy will be taken seriously and may result in disciplinary action up to and including dismissal for employees. For subcontractors or third parties, breaches may result in termination of contract and legal proceedings.

Where breaches involve criminal activity or serious misuse of data, Capital Sky may also report the matter to the relevant authorities.

Ongoing Obligations

The obligations contained in this policy continue even after an individual leaves Capital Sky Ltd. All confidential information remains the property of the company or its clients and must not be retained, shared, or used after employment or engagement has ended.

Policy Review

This policy will be reviewed annually, or sooner if required due to changes in legislation, cyber security requirements, operational practices, or industry standards.

Name: Martin Maloney

Position: Chief Executive Officer

Signature:



Dated: 15/05/2026

Latest Review Date: 15/05/2027