VERAXUS LTD

DATA PROTECTION POLICY

A practical policy for lawful, secure and responsible handling of personal data across Veraxus Ltd operations.

Company	Status	Effective date	Next review
Veraxus Ltd	Approved	08 May 2026	08 May 2027, or earlier if required

POLICY AT A GLANCE

Lawful and transparent	Limited and relevant
Personal data is processed only where Veraxus Ltd has a proper reason and can explain that purpose clearly.	Information collected is limited to what is needed for the relevant project, contract, legal or operational activity.
Secure handling - Records, documents, emails, site information and project evidence are protected using proportionate safeguards.	**Accountable governance** - Directors, managers and personnel are expected to handle information responsibly and raise concerns promptly.

CONTENTS

Controlled copy note: This document may be issued as a controlled PDF for client assurance, tender submissions, website download, internal governance and professional stakeholder review. Where a later signed copy is issued, the later signed copy takes precedence.

Document use

This policy is intended to support internal governance, client assurance, tender submissions and website publication. It should be read alongside project-specific confidentiality, contract and client data-handling requirements where those apply.

Publication note

The website presentation version may summarise this policy in plain language, but this official policy remains the controlled reference document for formal client, tender and governance use.

Plain language summary

Veraxus Ltd aims to keep personal information relevant, controlled, secure and used only where there is a proper business or legal reason.

1. INTRODUCTION

1.1 Responsible information handling: Veraxus Ltd recognises that personal data must be handled with care, control and accountability. The company is committed to processing information responsibly, lawfully and transparently, while keeping data protection standards proportionate to the size, nature and risk profile of the business.

1.2 Operational context: As a construction, refurbishment and operational delivery business, Veraxus Ltd may handle information relating to clients, suppliers, subcontractors, employees, professional contacts, residents, site visitors and other project stakeholders. This information may arise through enquiries, quotations, tender activity, site attendance, project evidence and routine business communication.

1.3 Trust and professional conduct: Information shared during business activity can be commercially sensitive, personally identifiable or operationally important. Data protection is therefore treated as part of wider project discipline, document control, communication standards, confidentiality and professional governance.

2. PURPOSE OF THIS POLICY

The purpose of this policy is to set a clear and practical framework for how Veraxus Ltd collects, uses, stores, shares, retains and disposes of personal data.

- **Legal compliance:** support compliance with applicable UK data protection legislation and recognised data protection principles.
- **Personal rights:** protect the rights and freedoms of individuals whose information may be processed during business operations.
- **Secure working:** maintain appropriate standards for controlled collection, storage, handling, sharing and disposal of information.
- **Risk reduction:** reduce the risk of accidental loss, unauthorised access, misuse, disclosure, alteration or destruction of personal data.
- **Client assurance:** demonstrate responsible governance consistent with contractor standards expected in commercial, residential, landlord, insurance, professional and public sector environments.

Policy position

This policy forms part of Veraxus Ltd's wider compliance and operational governance framework. It supports responsible document control, confidentiality requirements, project administration and secure communication across company activities.

3. LEGISLATIVE FRAMEWORK

Veraxus Ltd processes personal data in accordance with applicable UK data protection law, including UK GDPR, the Data Protection Act 2018, Privacy and Electronic Communications Regulations where applicable, and other relevant legal, contractual or regulatory requirements that may apply to specific business activities.

These requirements may apply to personal data in digital, paper, email, photographic, spreadsheet, cloud-based, portable storage, messaging or printed formats.

4. SCOPE OF THIS POLICY

This policy applies across Veraxus Ltd operations wherever personal data is processed. It covers personnel acting for or on behalf of the company, and it applies to business activities where personal information may reasonably be handled.

4.1 Personnel covered: Directors, employees, workers, temporary personnel, contractors, subcontractors, consultants, professional advisers and any other person processing personal data for Veraxus Ltd must follow relevant parts of this policy.

4.2 Business activities covered: The policy applies to client enquiries, quotations, tenders, contract administration, procurement, project coordination, access arrangements, supplier onboarding, employment administration, procurement records, health and safety records, commercial correspondence, business development, accounting, insurance and regulatory records.

4.3 Practical limits: This policy is intended to be proportionate. It does not replace project-specific confidentiality agreements, legal advice, contract terms, privacy notices, cookie notices or client-specific data handling requirements where those apply.

Page application note

For Veraxus Ltd, the practical test is simple: collect only what is needed, use it only for the purpose it was obtained, store it carefully, share it only where there is a proper reason, and review or dispose of it when it is no longer required.

5. KEY DEFINITIONS

Term	Meaning in this policy
Personal data	Information relating to an identified or identifiable living individual.
Processing	Any operation performed on personal data, including collection, use, storage, sharing, alteration, deletion or destruction.
Controller	The organisation that determines why and how personal data is processed.
Processor	A party that processes personal data on behalf of a controller.
Data breach	A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Special category data	Higher-risk personal information, such as health information, biometric data, trade union membership, racial or ethnic origin, religious beliefs or similar protected information.

Practical use: These definitions help personnel understand when ordinary project information becomes personal data and when stronger controls may be required.

6. DATA PROTECTION PRINCIPLES

Veraxus Ltd processes personal data in accordance with the core UK GDPR principles. These principles guide how information should be collected, used, stored, protected and reviewed.

Principle	How Veraxus Ltd applies it
6.1 Lawfulness, fairness and transparency	Personal data is processed only where there is a lawful basis and where processing can be explained clearly and fairly.
6.2 Purpose limitation	Personal data is collected for defined business, contractual, legal or operational purposes and is not used for unrelated or incompatible purposes.
6.3 Data minimisation	Only information necessary for the intended purpose is collected or used.
6.4 Accuracy	Reasonable steps are taken to keep personal data accurate and, where necessary, up to date.
6.5 Storage limitation	Personal data is not kept longer than reasonably required for the relevant purpose, legal duty or contractual requirement.
6.6 Integrity and confidentiality	Appropriate technical and organisational measures are used to protect data against unauthorised or unlawful processing, accidental loss, destruction or damage.
6.7 Accountability	Veraxus Ltd accepts responsibility for demonstrating compliance in a manner proportionate to its size, activities and risk profile.

Principle control note

These principles should be considered at the start of a project or administrative process, not only after records have already been created. They support proportionate data collection, controlled use, secure storage and accountable decision-making.

7. TYPES OF PERSONAL DATA PROCESSED

Veraxus Ltd may process the following categories of personal data where required for legitimate business purposes. The exact information processed will depend on the activity, project, relationship or legal requirement involved.

Category	Examples
Identification data	Full names, job titles, company affiliations, professional details and other information used to identify individuals in a business or project context.
Contact data	Telephone numbers, email addresses, postal addresses, communication preferences and related contact information.
Employment and workforce data	Recruitment records, right-to-work information, competency records, qualifications, insurance records, training records, site induction information and related personnel documentation.
Commercial and contract data	Information connected to contractual relationships, tendering, procurement, supplier engagement, project communication, quotations and commercial correspondence.
Site and project records	Site access details, attendance records, photographs, snagging records, inspection notes, handover records and project evidence where these contain personal information.
Technical data	Electronic records generated through routine business systems, such as email metadata, access logs, device information and system-generated operational records.
Special category or higher-risk data	Health, accident, absence, disability, reasonable adjustment, emergency contact or incident-related information where applicable and subject to stricter handling controls.

8. DATA COLLECTION

Personal data may be collected through ordinary business and project activity. Veraxus Ltd aims to collect information directly, clearly and only where it has a genuine purpose.

- **Client and project engagement:** enquiries, quotations, tenders, contract discussions, site meetings, instructions, project correspondence and handover records.
- **Supplier and subcontractor onboarding:** contact details, insurance information, competency evidence, procurement details and payment administration.
- **Employment and workforce administration:** recruitment records, right-to-work evidence, training, competency, attendance, accident and induction records.
- **Site and operational records:** access arrangements, photographs, inspection notes, project evidence, RAMS-related administration and health and safety records.
- **Routine correspondence:** emails, letters, telephone notes, messaging records and other communications required to administer business activity.

Data collection is limited to what is reasonably required for legitimate operational, contractual, legal or business purposes.

Collection control note

The company should avoid collecting excessive information at enquiry, tender, supplier onboarding or site stage. Where a photograph, email or form is not needed for a real project or business purpose, it should not be retained simply because it is available.

9. LAWFUL BASES FOR PROCESSING

Veraxus Ltd will identify an appropriate lawful basis before processing personal data. Depending on the circumstances, the company may rely on one or more of the following lawful bases.

Lawful basis	Example application
Contract	Processing required to enter into, manage, perform or administer a contract, quotation, tender, project instruction, purchase order or supplier relationship.
Legal obligation	Processing required to comply with law, including employment, accounting, tax, company, health and safety, insurance, regulatory or record-keeping duties.
Legitimate interests	Processing required for proportionate business interests, such as project delivery, client communication, supplier management, evidence records, debt recovery, commercial administration and business development.
Consent	Processing based on clear consent where this is appropriate and where consent can be freely given, withdrawn and recorded.
Vital interests or public task	Processing that may apply only in limited circumstances, such as emergency situations or where required by a public authority context.

Special category data

Where special category or higher-risk information is processed, Veraxus Ltd will ensure that an additional condition for processing applies and that stronger safeguards are used where required.

10. DATA USE

Personal data is used only where it supports a legitimate business, contractual, legal or operational purpose. It will not be used for unrelated or incompatible purposes unless there is a valid lawful reason to do so.

- **Contract administration:** preparing quotations, responding to tenders, managing works, issuing project records and maintaining commercial correspondence.
- **Project coordination:** arranging site access, scheduling works, communicating with clients, subcontractors, residents, suppliers and professional teams.
- **Supplier engagement:** checking supplier details, arranging orders, managing contact records and processing relevant commercial documentation.
- **Employment administration:** managing recruitment, competency, right-to-work, training, induction and personnel records.
- **Legal compliance:** meeting health and safety, tax, accounting, insurance, regulatory, contractual and record-keeping obligations.
- **Operational delivery:** maintaining appropriate records to evidence progress, quality, attendance, instructions, variations, handover and issue resolution.

Use control note

Personal data should remain connected to the purpose for which it was obtained. If information is later needed for a different purpose, personnel should consider whether that use is compatible, necessary and proportionate before proceeding.

11. SITE PHOTOGRAPHS, PROJECT EVIDENCE AND COMMUNICATIONS

Veraxus Ltd may use photographs, videos, messages, emails and project records as part of construction, refurbishment and operational evidence. These records may support surveys, progress reporting, quality control, variations, snagging, handover, tender evidence, dispute avoidance, client communication or case study preparation.

Where such records contain personal data, Veraxus Ltd will apply proportionate care. This includes:

- **Relevant records only:** capturing and retaining photographs or communications only where they support a genuine business or project purpose.
- **Avoid unnecessary personal exposure:** avoiding unnecessary inclusion of identifiable individuals, private information, personal belongings, sensitive documents or non-relevant areas where reasonably possible.
- **Controlled sharing:** sharing project images and records only with relevant parties where there is a proper operational, contractual or commercial reason.
- **Evidence handling:** treating project evidence, client comments, WhatsApp screenshots, emails and related records as controlled business records.
- **Website and marketing use:** using project images or case study materials carefully, with redaction or anonymisation where required and with client permissions where appropriate.

Construction-specific control

Photographs and messages can be valuable evidence, but they should show the work, condition, defect, progress or handover point - not unnecessary personal details.

12. DATA STORAGE AND SECURITY

Veraxus Ltd applies proportionate technical and organisational measures to protect personal data, including controlled access, device protection, secure paper storage, careful email/document sharing, cloud account controls, staff awareness and secure disposal.

- **Access control:** password-protected systems and controlled access to records based on operational need.
- **Device and account security:** sensible protection for company equipment, accounts and business systems.
- **Paper and document care:** secure storage, careful sharing and appropriate disposal when records are no longer required.
- **Cloud and system controls:** use of appropriate business systems, account ownership, confidentiality and continuity safeguards.

Secure handling summary

Project records, photographs, emails and site notes should be handled as controlled business material. Where files are shared externally, the recipient, purpose, content and method of sharing should be considered before release.

13. DATA SHARING AND THIRD-PARTY PROCESSORS

Data sharing means providing personal data to another person or organisation. Third-party processors are organisations that process personal data on behalf of Veraxus Ltd, such as accountants, cloud systems, professional advisers, payroll support, document platforms or other service providers.

13.1 When sharing may be necessary: Veraxus Ltd may share limited personal data where it is necessary for legitimate business, contractual, legal or operational purposes. This may include professional advisers, accountants, legal representatives, insurers, approved suppliers, subcontractors, clients, principal contractors, regulators or public authorities.

13.2 Controlled and limited sharing: Information will be shared on a need-to-know basis and only to the extent reasonably required. Personnel should consider whether the recipient is appropriate, whether information is relevant, whether unnecessary details can be removed and whether the transfer method is suitable.

13.3 Processors and safeguards: Where a third party processes personal data on behalf of Veraxus Ltd, reasonable checks will be undertaken to confirm that appropriate safeguards are in place. This may include contractual terms, account controls, confidentiality obligations, service provider reputation or proportionate assurance measures.

Controlled sharing	Avoidable sharing
Sending subcontractor insurance information to a principal contractor; providing payroll or accounting records to an accountant; passing relevant access details to an approved project party.	Sending full documents where only an extract is needed; forwarding email chains containing unrelated personal details; sharing photographs where a cropped or redacted image would be sufficient.

14. INTERNATIONAL TRANSFERS AND CLOUD-BASED SYSTEMS

Veraxus Ltd may use reputable digital, email, website, storage, accounting or document-management systems. Some providers may store or access data outside the United Kingdom or use international technical infrastructure.

- **Reasonable assurance:** where international transfers are relevant, Veraxus Ltd will seek to rely on appropriate legal mechanisms, provider safeguards, contractual arrangements or recognised transfer protections where required.
- **Business systems:** systems should be selected and managed with attention to security, access controls, account ownership, confidentiality and continuity of records.
- **Sensitive material:** higher-risk information should not be uploaded, forwarded or shared unless there is a genuine business purpose and a suitable route for doing so.

15. DATA RETENTION AND SECURE DISPOSAL

Personal data is retained only for as long as reasonably required. Records may be kept for legal obligations, contractual requirements, project evidence, warranties, disputes, supplier history, tender evidence, case studies and controlled business growth. Data no longer required should be securely deleted, destroyed, archived, anonymised or otherwise managed in a controlled way.

Sharing and retention control note

Before sharing or retaining information, personnel should consider necessity, audience, sensitivity, retention need and whether redaction or anonymisation would achieve the same purpose with lower risk.

16. INDIVIDUAL RIGHTS

Individuals have legal rights in relation to their personal data. These rights apply subject to legal conditions, exemptions and the specific circumstances of the request.

Right	Summary
Access	Individuals may request confirmation of whether personal data is being processed and receive a copy of relevant personal data.
Rectification	Individuals may request correction of inaccurate or incomplete data.
Erasure	Individuals may request deletion of personal data where lawful and applicable.
Restriction	Individuals may request limited processing in certain circumstances.
Objection	Individuals may object to processing where applicable.
Portability	Individuals may request transfer of data where applicable.
Withdraw consent	Where processing is based on consent, individuals may withdraw consent where processing relies on that consent.

All requests will be handled in accordance with applicable legal timeframes and requirements.

17. SUBJECT ACCESS REQUESTS

Subject access requests and other data rights requests should be submitted in writing to Veraxus Ltd. Requests are normally responded to without undue delay and within one month, subject to lawful extensions where applicable.

- **Clear requests:** a request should identify the individual and explain the information being requested so that relevant records can be located.
- **Identity verification:** Veraxus Ltd may request proof of identity or further clarification where this is necessary and proportionate.
- **Complex requests:** where a request is complex or numerous, the response period may be extended where permitted by law and the individual will be informed.
- **Third-party information:** information relating to other individuals, confidential commercial information or legally privileged material may need to be reviewed before disclosure.

Request handling note

Rights requests should be logged, acknowledged and assessed carefully. The company should identify the requester, locate relevant records, consider third-party information, and keep a proportionate record of the response decision.

18. DATA BREACH MANAGEMENT

Veraxus Ltd treats all suspected personal data breaches seriously. Potential breaches may include unauthorised access, loss or theft of documents or devices, disclosure to an unintended recipient, cyber incident, email misdirection, data corruption or accidental destruction of records.

Where a breach or suspected breach is identified, Veraxus Ltd will follow a structured response:

Response stage	Action
1. Assess the incident	Identify what happened, when it happened, what data may be involved and who may be affected.
2. Contain the issue	Take immediate steps to limit further exposure, recover information or secure affected systems.
3. Investigate	Review the circumstances, root cause, affected records and any continuing risk.
4. Record the decision-making	Keep a proportionate breach log, including what happened and what action was taken.
5. Determine reporting duties	Consider whether the incident is notifiable to the ICO or affected individuals.
6. Correct and improve	Apply corrective actions, improve controls and reinforce relevant awareness.

Breach reporting threshold

Not every incident has to be reported to the ICO. Veraxus Ltd assesses whether the incident is likely to result in a risk to individuals' rights and freedoms and keeps appropriate records of the assessment and response.

19. STAFF AWARENESS AND GOVERNANCE

Veraxus Ltd promotes practical awareness through clear expectations, management oversight and proportionate controls. Personnel handling information are expected to use data only where necessary, maintain confidentiality, control project records, escalate concerns promptly and support management review as the business grows.

20. COMPLAINTS

Concerns regarding data handling should first be directed to Veraxus Ltd so that the matter can be reviewed and addressed. Individuals may also contact the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, or through www.ico.org.uk.

Incident and complaint record

Where an issue, complaint or incident is raised, Veraxus Ltd should keep a clear record of the concern, the information involved, actions taken, decisions made, any reporting assessment and any improvement identified.

21. MONITORING AND CONTINUOUS IMPROVEMENT

Veraxus Ltd recognises that data protection is an evolving compliance area. The company is committed to reviewing procedures and improving controls where appropriate.

- **Periodic review:** procedures will be reviewed to ensure they remain suitable for the company's work and risk profile.
- **Operational learning:** feedback, incidents, near misses, client requirements and project experience will inform improvements.
- **Business growth:** systems and controls will be adapted as the company grows, handles more records or uses additional platforms.
- **Legal alignment:** this policy will be updated where required following relevant legal, regulatory or operational change.

22. POLICY REVIEW

This policy will be reviewed annually and earlier where required. Review may be triggered by legislative or regulatory change, operational change, significant organisational change, a significant data incident, new systems or suppliers, or the identification of improvement opportunities.

Review approach

The review is intended to keep the policy practical, proportionate and suitable for Veraxus Ltd's construction, refurbishment, tendering, project administration and business governance activities.

Approval context

The approval section below confirms that this policy has been adopted for company governance, client assurance and operational use. It is not intended to replace client-specific data protection terms where a project contract requires a different process.

23. DECLARATION AND ELECTRONIC APPROVAL

This policy is approved by Veraxus Ltd and applies across company operations. It is intended to support responsible data handling, client assurance, tender readiness, internal governance and professional standards.

Application area	Approval meaning
Company governance	The policy sets the expected standard for how Veraxus Ltd handles personal data during ordinary business activity.
Client and tender assurance	The policy may be issued to clients, advisers, contractors, portals and stakeholders as evidence of controlled information handling.
Operational use	Personnel should use this policy when handling project records, site information, supplier details, emails, photographs and employment records.
Future improvement	The policy will be reviewed as systems, records, legal duties, tender requirements and business operations develop.

Approval statement: Approved and signed electronically on behalf of Veraxus Ltd. This document has been electronically approved and signed by the Director of Veraxus Ltd. The typed signature below is intended to authenticate and approve this document on behalf of the company.

Approval item	Detail
Name	Alex Stefan
Position	Director
Signature	Alex Stefan
Date	08 May 2026
Document status	Approved
Next review	08 May 2027, or earlier if required
Approval control	**Practical meaning**
Authority	The policy is approved for use as a Veraxus Ltd company governance and client assurance document.
External issue	The document may be supplied to clients, advisers, contractors, portals and professional stakeholders where evidence of data protection governance is required.
Operational use	Personnel should apply the policy when handling emails, site photographs, project records, supplier information, subcontractor details and employment records.
Review control	Any future update should be issued as a replacement controlled policy rather than informal amendment to the approval page.
Final control check	**Expected standard**
Complete document	The policy should be issued as a complete PDF so that wording, approval and review information remain together.
No informal edits	Externally issued copies should not be altered without replacing the full controlled policy.
Review trigger	A review should be considered after material system, supplier, tender, legal, operational or incident-related change.
Responsible ownership	Directors retain overall responsibility for ensuring the policy remains suitable for the company's operations.

Approval control note

This approval confirms the policy standard at the date shown. The document should be reviewed when systems, legal requirements, tender requirements, business processes or operational risks materially change.

Controlled document note

When issued externally, this policy should be treated as a controlled business document. Any future update should be issued as a replacement policy rather than by informal amendment to the signed approval page.

Website and tender use note

A plain-language website summary may be used for visitors, but where a client, adviser or tender portal requires formal evidence, this signed policy PDF should be provided as the authoritative document.

Completion note

This policy has been prepared as a formal, electronically approved document for controlled use by Veraxus Ltd.