DATA PROTECTION POLICY STATEMENT

Vista Civil Engineering Limited is a business that seeks to achieve and maintain excellence in all that we do, in particular the protection of data. We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. We are registered with the Information Commissioner's Office (ICO) and are fully committed to complying with data protection laws and ensuring the security of personal data. We are also accredited to Cyber Essentials.

Our policy sets out how we seek to protect personal data and ensure that staff understand the rules governing the use of personal data to which they have access in the course of their work. This policy requires staff to consult with the directors before initiating any new significant data processing activity is initiated and that relevant compliance steps are addressed.

The purposes for which personal data may be used by us:

BUSINESS
Personnel, administrative, financial, regulatory, payroll and business development.

- Compliance with our legal, regulatory, and corporate governance in line with good practice.
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.
- Ensure business policies, such as internet use, are complied with.
- Operational reasons include recording transactions, training, and quality control.
- Managing complaints.
- Checking references, ensuring safe working practices, monitoring, and managing staff.

PERSONAL DATA
Information relating to identifiable individuals which may include:

- Contact details.
- Educational background.
- Financial and pay details.
- Details of certificates and diplomas.
- Education and skills.
- Marital status.
- Nationality.
- Job title.
- Curriculum vitae.

SENSITIVE PERSONAL DATA
Sensitive Personal Data refers to information relating to identifiable individuals, which may include:

- Race or ethnic origin.
- Political opinions.
- Religious or similar beliefs.
- Trade union membership.
- Physical or mental health or condition.
- Criminal offences or related proceedings.

SCOPE
This policy applies to all staff, and all staff must be familiar with the content and comply with the terms. The Company Secretary has overall responsibility for the day-to-day implementation of the policy.

PROCEDURES AND RESPONSIBILITIES
We will process personal data fairly and lawfully in accordance with individual's rights. This generally means that we should not process data unless the individual whose data we are processing has consented to or there is a legitimate business compliance purpose.

The ultimate responsibilities of the Company Secretary and Board of Directors are:

- Keeping the board up to date about data protection responsibilities, risks, and issues.
- Reviewing data protection policies and procedures on a regular basis.
- Arranging data protection training and advice for all staff.
- Answering data protection questions from all staff and the board.
- Responding to individuals who wish to know what data is being held by VISTA.
- Checking and approving any third-party companies that hold information the company is responsible for.
- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third party services, such as cloud services, the company is considering using to store or process data.
- Approving data protection statements attached to emails or other marketing materials e.g. website.
- Addressing data protection enquiries from clients, target audiences or media outlets.
- Coordinating with the Marketing to ensure all marketing initiatives adhere to data protection laws and the company's data protection policy.

All Employees

- Ensure data does not remain available to others whilst they are away from their desk
- Ensure computers, laptops, tablets, and smartphones are locked when they are not in use and away from the individual user
- Communicate any concerns over a breach of data protection

The processing of data must be relevant to deliver our services, in our legitimate interests so as not to prejudice the individual's privacy. In most cases this provision will apply to routine business activity. Any activity outside of this scope must first be approved by the Company Secretary before being processed.

PRIVACY NOTICE
Our privacy notice

- Sets out the purpose for which we hold personal information on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisors
- Informs customers they have a right to access the personal data that we hold on to them
- Vista will not sell any information to a third party for marketing purposes.

ACCURACY AND RELEVANCE
We will ensure that any personal data we process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. We will not process data for any purpose other than being explained and intended without prior consent of the individual or it would be reasonable to expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe the information provided is inaccurate you should speak to the Company Secretary for advice on the next steps i.e. dispute.

You are responsible for ensuring the information we hold on you is relevant and up to date. For example, if your personal details change, you must inform the relevant individual so records can be updated.

SECURE STORAGE

- In cases when data is stored on printed paper it will be kept in a secure place where unauthorised individuals cannot access it.
- Printed data will be shredded when it is no longer needed and disposed of appropriately
- Data stored on computers or in the cloud will be stored securely (e.g., in hidden folders, password-protected folders), with restricted access and communication of passwords strictly maintained.
- The server containing personal information will be protected in a secure location and kept away from general office locations
- Data will be backed up regularly in accordance with IT procedures
- Data should never be directly saved to computer or laptops, desktops, tablets, or smartphones
- All devices storing sensitive data must be authorised and secured with appropriate software and antivirus protection.

DATA RETENTION

Data will not be retained longer than is necessary for the purposes for which it was collected. Any information retained will depend on circumstances and in each case the reasons why are taken into account. Where this is the case the Company Secretary will be consulted.

SUBJECT ACCESS REQUESTS

Any request for personal data must be authorised by the Company Secretary, who will review the request in line with applicable data protection laws. Each case will be reviewed individually under the circumstances under which the information has been requested. There may be restrictions on the information to which you are entitled by law.

Personal information will not be transmitted outside of the European Economic Area.

TRAINING

All staff will receive training on this policy. New joiners will receive training as part of the induction process; further training will be provided on an ad-hoc basis. Training is provided in-house, and it will cover the law relating to data protection and related policies and procedures. The completion of training is compulsory for all employees.

CONDITIONS FOR PROCESSING

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of privacy notice.

- What is being collected?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- Identify and contact details of any controllers
- Retention period

JUSTIFICATION FOR PERSONAL DATA

We will process personal data in compliance with the 7 key principles set out by GDPR, these are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

We will document any additional justification for the processing of sensitive data and ensure any biometric and genetic data is considered sensitive.

CRIMINAL RECORD CHECKS
Any criminal record checks are justified by law and relevant. Criminal record checks will not be undertaken solely based on the consent of the subject.

DATA PORTABILITY
Upon request a data subject will have the right to receive a copy of their data in a structured format. These requests will be processed within one month, provided there is no undue burden and does not compromise the privacy of other individuals or affect legal proceedings. There will be no charge for this information.

RIGHT TO BE FORGOTTEN
Anyone may request that their data is disposed of, deleted or removed. Any third parties with access to this information must comply with this request. A request under these circumstances may only be refused if a specific exemption under data protection laws applies. Each case should be reviewed individually.

DATA AUDITS
Regular audits will be undertaken to manage and mitigate risks under data protection and the results recorded. This process contains information on what data is held, where it is stored, how it is used, who is responsible, who has access and further regulations on retention timescales that maybe relevant.

REPORTING BREACHES
All members of staff have an obligation to report actual or potential data protection compliance failure. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Report breaches to the Information Commissioners Office.

We take compliance with this policy very seriously. Failure to comply can put the organisation and individuals at risk. Failure to comply with this policy may result in disciplinary action, up to and including dismissal.

Signed

For and on behalf of Vista Civil Engineering
Bradley Hewitt
Director

Date May 2026

Review Date May 20267