The Martin Group of Companies

Incorporating:

HW Martin Holdings Limited

HW Martin Fencing and Forestry Limited

HW Martin Traffic Management Limited

HW Martin Safety Fencing Limited

HW Martin Fleet Maintenance Limited

HW Martin Waste Limited

Amber Langis

Premier Waste Recycling Limited

Lochrin Bain Limited

King Vehicle Engineering Limited

King Trailers Limited

King Transport Equipment Limited

King Highway Products Limited

Safety Vehicle Hire and Lease Limited

Virtus Traffic Management Solutions Limited

Group Data Protection Policy

Document History

Written by	Libby Reed	
Authorised by	James Clegg	

Review Date	Reviewed By		Comments / Amendments	Version
25 June 2025	Libby Reed		Annual review. Major changes to structure & wording. Contents page added. References updated. Sections expanded including 'rights' and responsibilities. Complaints section added. Change signatory.	2.0
28 June 2024	Jim Clegg		Annual review.	1.5
26 February 2024	Gavin Peace		Interim review to reflect authorization name change.	1.4
30 April 2023	Gavin Peace		Annual Review. Virtus Traffic Management Solutions Limited added. Data Subject Access Requests – Third Parties section added. data@hwmartin.com added for contact and queries.	1.3
30 April 2022	Iain Kay		Annual review. No changes.	1.2
30 April 2021	Iain Kay		Annual review. No content changes. New logo added.	1.1
30 April 2020	Iain Kay		Annual review and change to document reference in line with MSV 03-1-3 Procedure for Documented Information	1.0

Contents

1. Introduction & Purpose

The Martin Group of Companies is committed to protecting the rights and freedoms of data subjects by safely and securely processing their data in accordance with all our legal obligations including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
We hold personal data about our employees, clients, customers, suppliers and other individuals for a variety of business purposes.

This policy operates within the framework of the Martin Group's Information Security Management System (ISMS) which is aligned to the principles of ISO/IEC 27001 and outlines how we protect personal data held about our employees, clients, customers, suppliers, and other individuals for various business purposes, ensuring our staff understand the rules for its use. Staff must ensure appropriate planning for any significant new data processing, including assessing the need for a Data Protection Impact Assessment (DPIA) to manage risks to privacy.

This policy is applicable to everyone and must be observed by all employees. The board will keep this policy under review and update, amend or re-issue it as required.

2. Scope

This policy applies to all staff, including employees, contractors, temporary staff, and any other individuals who access or process personal data on behalf of the Martin Group of Companies. All such individuals must be familiar with and comply with its content.

This policy supplements other policies relating to processing activities, such as the use of surveillance systems and Information and Communications Technology (ICT), as well as procedures within our Information Security Management System (ISMS). It should be read alongside these documents to support a full understanding of how we protect information, including personal data

We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be communicated to staff prior to implementation.

3. Definitions

Business purposes	The purposes for which personal data may be used by The Martin Group include the following: • Performing the functions and operations required for the successful and efficient day-to-day running of our businesses, operating companies, contracts and projects • Compliance with our legal, regulatory and corporate governance obligations and good practice • Ensuring business policies are adhered to (such as those covering the use of email and the internet) • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • The investigation of complaints • Operational functions such as the recording of transactions, managing training, quality control, safeguarding the confidentiality of commercially sensitive information, security vetting, reference checking and credit scoring / checking

	• Ensuring safe working practices, monitoring and managing staff access to systems / facilities, managing staff absences and conduct, disciplinary matters and administration • Marketing and business development Improving the services we offer and expansion into new markets
Personal data	Personal data means any information relating to an identified or identifiable person ("data subject"). An identifiable person is anyone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. We gather personal data in relation to the business purposes outlined above. Examples of personal data we gather include (but are not limited to) the following: • contact information (such as address, phone, email) • details of education, employment history, training, qualifications, certifications and curriculum vitae • nationality and evidence of an individual's right to work in the UK • payroll information (such as bank details, NI number, tax coding) • information related to the driving of vehicles on company business (such as driving licenses, records of driving hours and tachographs) • information relating to medical or occupational health assessments, drugs and alcohol testing, illness and absences from work • information relating to work-related accidents and incidents information about third parties (non-employees) for the purposes of undertaking our legal, regulatory or contractual obligations
Special categories of personal data	Special categories of personal data cover subjects that are more sensitive and therefore require additional protection. This type of data could create significant risks to an individual's fundamental rights and freedoms, for example by placing them at risk of unlawful discrimination. The special categories include information about an individual's: • race • ethnic origin • political beliefs • religion • trade union membership (or non-membership) • genetics • offences or potential offences • biometrics (where used for ID purposes) • health • sexual orientation
Data controller	Data controller means the person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means by which personal data is processed, where the purposes and means of such processing are determined by law.

Data processor	Data processor means a person, public authority, agency or other body that processes personal data on behalf of a data controller.
Processing	Processing means any operation(s) performed on personal data by manual or automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	The national body responsible for data protection and supervisory authority for our organisations is the Information Commissioners Office (ICO).
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

4. Responsibilities

4.1 All Staff

Each member of staff is responsible for understanding and implementing the Group Data Protection Policy. They must follow its principles in all data-related activities.

4.2 Line Managers

Line Managers are accountable for ensuring their team members:

- Understand and follow the Group Data Protection Policy.
- Complete any Company-provided data protection training as required.

4.3 Information Security / Data Protection Manager (ISM/DPM)

This role is responsible for overseeing both data protection and information security across the organisation. Key responsibilities include:

- Advising the board and senior leadership on data protection and information security matters.
- Developing, reviewing, and implementing relevant policies and procedures.
- Providing training, guidance, and support to staff on data protection and security best practices.
- Monitoring compliance with data protection laws and information security requirements.
- Managing data protection and information security risks, including responding to incidents and breaches.
- Overseeing Data Protection Impact Assessments (DPIAs).
- Cooperating with the Information Commissioner's Office (ICO) as required.
- Promoting a strong culture of information security throughout the business.

4.4 Senior Information Security Team

This team (heads of HR, IT, Finance, etc.) ensures their departments comply with data protection and information security standards.

- Collaborating with the ISM/DPM to ensure that information security policies are properly implemented within their departments.
- Assisting the ISM/DPM in identifying potential risks to personal data within their areas of responsibility.
- Ensuring that employees in their departments are trained on data protection and security policies and practices.
- Overseeing the secure handling, storage, and processing of personal data in accordance with company policies.

- Coordinating responses to data security incidents and breaches within their departments and informing the ISM/DPM.

4.5 Information Security Champions

Designated individuals in each subsidiary, responsible for data protection liaison within their company.

- Acting as the primary point of contact for information security and data protection issues within their subsidiary.
- Collaborating with the ISM/DPM to ensure their subsidiary complies with the information security policies and laws.
- Promoting awareness of information security and data protection practices within their subsidiary, ensuring that all employees understand and follow the policies.
- Assisting with the implementation of technical and organisational measures to safeguard personal data and ensure compliance with the Data Protection Policy.
- Reporting any security incidents or breaches involving personal data to the ISM/DPM, following the company's procedures for incident response.
- Monitoring and reviewing information security practices within their subsidiary, escalating concerns to the ISM/DPM.

4.6 ICT Manager

The ICT Manager is responsible for:

- Ensuring 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.

4.7 Data Controllers

Data controllers are responsible for:

- The analysis and documentation of the type of personal data we gather and process.
- Checking procedures to ensure all rights of individuals and data subjects are appropriately covered.
- Ensuring data is stored in a safe and secure manner.
- Identifying the lawful basis for processing and gathering data.
- Ensuing procedures for obtaining consent are suitable, sufficient and lawful.
- Implementing and reviewing procedures to detect, report and investigate personal data breaches.
- Assessing the potential risks posed to individual rights and freedoms should any breaches of personal data occur.

4.8 Data Processors

Data processors are responsible for:

- Ensuring they fully understand their data protection obligations.
- Checking that any data processing activities they are dealing with comply with this policy.
- Ensuing that data is not used in any unlawful way or in a manner that breaches this policy
- Ensuing data is stored correctly and processed carefully and accurately.
- Raising any concerns, notifying any breaches or errors and reporting anything suspicious or contradictory to this policy or our legal obligations without delay to the appropriate data controller.

5. Data Protection Principles

The Martin Group will comply with the data protection principles as set out in the UK GDPR and the DPA 2018. These principles are:

5.1 Lawfulness, Fairness, and Transparency

Data collection will be fair, for a legal purpose, and we will be open and transparent as to how the data will be used.
We will identify a lawful basis before processing any personal data. We will provide clear and comprehensive privacy notices to data subjects (see Section 10) at the time of data collection or as soon as reasonably practicable.

5.2 Limited for its Purpose:

Data will only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
We will ensure that data is collected only for the purposes outlined. Any new purpose for processing will be assessed for compatibility, and consent will be obtained if required.

5.3 Data Minimisation

All data collected will be strictly necessary and not excessive for its purpose.
We will regularly review our data collection practices to ensure that we only collect the minimum amount of personal data required for the specified purpose.

5.4 Accuracy

The data we hold will be accurate and kept up to date.
We will implement procedures to ensure data accuracy, including providing data subjects with the opportunity to update their information and regularly reviewing data for inaccuracies.

5.5 Storage Limitation

We will not store data for any longer than necessary.
We will adhere to our data retention policy, which sets out specific retention periods for different categories of data.

5.6 Integrity and Confidentiality

We will ensure data we hold is kept safe and secure.
We will implement appropriate technical and organisational measures to protect personal data, as detailed in our ISMS policies.

5.7 Accountability

The data controller shall be responsible for, and be able to demonstrate compliance with, these principles.
We will maintain a data register, conduct regular audits, provide data protection training, and document our processing activities to demonstrate compliance.

6. Individual Rights

Under the UK GDPR, individuals have several rights regarding their personal data. The Martin Group is committed to upholding these rights through proactive measures and by responding appropriately when individuals exercise them. While some rights are fulfilled automatically — such as providing clear privacy notices — others may involve direct requests from individuals. When a request is made

(e.g. to access, rectify, or erase data), it should be directed to the ISM/DPM and will typically be responded to within one calendar month.

6.1 Right to be informed

Individuals have the right to be informed about how their personal data is collected and used. We provide this information through our privacy notices, which are clear, concise, and issued either at the point of data collection or within one month if the data is obtained from a third party.

6.2 Right of access

Individuals have the right to access the personal data we hold about them. This is commonly referred to as a Subject Access Request (SAR). The Martin Group has a documented procedure (GRP-ISMS-PRO-001) for handling SARs, which ensures all requests are dealt with lawfully and within the timeframes set out under UK GDPR.

6.3 Right of rectification

If an individual believes their personal data is inaccurate or incomplete, they have the right to request that it be corrected or completed without undue delay. If the data has been disclosed to third parties, we will take reasonable steps to inform them of the rectification, where this is possible and lawful to do so.

6.4 Right to erasure

Also known as the 'right to be forgotten', individuals may request the deletion of their personal data in specific circumstances, such as when it is no longer necessary for the purpose it was collected. This right is subject to exemptions (e.g. legal obligations, public interest, legal claims).

6.5 Right to restrict processing

Individuals can request a temporary restriction on the processing of their personal data in certain circumstances, such as when the right to rectification is being exercised. Where processing is restricted, the data will be clearly marked and only processed under limited conditions.

6.6 Right to data portability

Where processing is based on consent or contract and carried out by automated means, individuals can request to receive their personal data in a structured, commonly used, and machine-readable format, and have it transferred to another controller where technically feasible.

6.7 Right to object

Individuals can object to the processing of their personal data where it is based on our legitimate interests or used for direct marketing. Processing will cease unless we can demonstrate compelling legitimate grounds to continue.

6.8 Rights related to automated decision-making including profiling

Individuals have rights where decisions are made solely through automated processing, including profiling. In such cases, we will implement appropriate safeguards to protect their rights, including the right to obtain human intervention, express their point of view, and contest the decision.

It is essential that staff understand the rights individuals have under data protection law. This section provides a summary of those rights, but for further detail, staff should refer to the ICO's guidance on individual rights or seek advice from the ISM/DPM. Internal training and guidance materials are also available to support understanding and handling of rights requests.

7. Complaints

Employees who have concerns about how their personal data is being handled, or who feel their rights under data protection law are not being respected, can raise a complaint by contacting the ISM/DPM at data@hwmartin.com. We will handle complaints in line with our obligations under data protection law and respond within one calendar month of the complaint being received.

If the individual remains dissatisfied, they have the right to raise their concern with the ICO.

8. Special Categories

We will seek each individual's explicit consent to process data that falls into special categories, unless exceptional circumstances apply, or we are required to do so in order to comply with the law (e.g. to ensure compliance with the Health and Safety at Work Act). Such consent will clearly identify what the relevant personal data is, why it is being processed and to whom it will be disclosed. Any processing of special categories of personal data that takes place without this consent will be stopped immediately and reported as a breach.

9. Criminal Offence Data

We will only undertake criminal record checks where they can be lawfully justified. Checks will not be undertaken based only on the consent of the data subject. We will not keep registers of criminal offence data. All data relating to criminal offences will be treated as a special category of personal data.

10. Subject Access Requests

Requests for access to personal data (Subject Access Requests) are handled in accordance with our separate Subject Access Request Procedure as mentioned in section 6.2. The following sections provides an overview of individual and third-party entitlements under UK GDPR.

10.1 Data Subject Access Requests – Employees

An individual has the right to receive confirmation that their data is being processed, access to their personal data and any supplementary information. We will provide an individual with a copy of the information they request, free of charge. This will occur without delay, and within one month of their request being received. We will provide data subjects with access to their information in commonly used electronic formats. If complying with a request is complex or multifaceted, the timescale for responding may be extended to three months with approval from the relevant Data Controller. The individual must be informed of this extension within one month of their original request being received. Following the receipt of a subject access request, we will ensure that the data requested is not altered or amended in any way.
We retain the right to refuse to respond to certain requests and may choose, in circumstances of the request being manifestly unfounded or excessive, to charge a fee. If the request is for a large quantity of data, we will request that the individual specify precisely the information they are requesting.

10.2 Data Subject Access Requests – Third Parties

(For example the police, Solicitors, mortgage application salary details, home rental references etc): If a third party makes a request on behalf of an employee, ex-employee or customer/client and they enclose a recently signed authority then this request is to be treated the same way as if it had been requested by an individual.

If you receive a request from the police or another enforcement agency who are acting to detect or prevent crime, then you must consult with the Group ISM/DPM at data@hwmartin.com before any information is released. If information is to be released, then the requester must first complete and provide GRP-ISMS-FOR-001a Subject Access Request From. The ISM/DPM will deal with such requests.
Some governmental agencies have a legal right to access information without the need for consent (e.g., Child Support Agency). These requests should be dealt with on a case-by-case basis and referred to the ISM/DPM for consideration.

11. Privacy Notices

Privacy notices will be supplied at the time we obtain personal data, if the data is being obtained directly from the individual. If the data is not obtained directly from the individual, then we will provide a privacy notice within one month of the data being obtained. Where we envisage data being disclosed to another recipient, we will provide a privacy notice prior to the data being disclosed.
Our privacy notices will be concise, transparent, intelligible and easily accessible. They will be provided free of charge and written in clear, plain language. We will include the following information in privacy notices to all data subjects:

- The identity and contact details of the employer;
- A description of the personal data that is collected;
- The purposes for processing the data;
- The legal basis on which the processing will take place;
- Who the personal data is shared with;
- Whether personal data is transferred outside of the EEA and if so, details of the safeguards that are in place to protect the security of the data;
- How long the personal data will be kept for; and
- Details about the rights that employees have in relation to that personal data, for example the right to request that the employer rectify any incorrect information.

12. Data Sharing & Transfer

Information sharing must be carried out in accordance with the UK GDPR, the DPA 2018, and our Information Sharing Policy. Failure to do so could result in non-compliance or a data breach.

13. Procedures

The procedures contained within each operating companies Integrated Management Systems will ensure we act with confidentiality, integrity and transparency in all our use of personal data and demonstrate how we will comply with each of the principles mentioned in section 5 of this document. Data Controllers and processors will work together to generate DPIA's in line with our Data Protection Impact Assessment procedure, for high-risk areas and maintain written records of how our data processing activities are lawful and compliant with UK GDPR and DPA 2018. Our Group Article 30 Register of Processing Activities Statement contains details of the data we collect, how it is collected, how it is used and who by and how it is stored and secured. It identifies the high-risk areas that require DPIA's to be generated. The Register of processing activities will be reviewed and updated annually with this policy, and as required due to changes in legislation or the activities being undertaken by any of the Group companies.

14. Third-Party Data Controllers and Processors

We will have written contracts in place with any third-party data controllers and / or processors that we use or have need to interact with. This includes the transfer of personal data to our clients and potential clients for the purposes of demonstrating our competence and ability to discharge our contractual obligations. The contracts will contain specific clauses that set out the liabilities, obligations and responsibilities of each party. As a data controller, we will only appoint processors who can provide sufficient guarantees under UK GDPR and that the rights of data subjects will be respected and protected. As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under UK GDPR and we will protect and respect the rights of data subjects.

Our contracts will comply with the standards set out by the Information Commissioners Office and, where possible, follow the standard contractual clauses which are available. Our contracts with other data controllers and / or data processors will set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

As a minimum, our contracts will include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Processors will only be engaged with the consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under UK GDPR
- The processor will assist the controller in meeting its UK GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on UK GDPR.

15. Data Breach Reporting and Management

The Martin Group has a legal obligation to report any data breaches to the Information Commissioners Office within 72 hours. Any breaches of this policy, our procedures or data protection laws must be reported to the appropriate Data Controller and the Group Information Security Manager as soon as any employee becomes aware of a breach. The prompt reporting of actual or potential data protection compliance failures is vital to ensure we can:

- Investigate the non-compliance and take remedial action where necessary
- Maintain a register of compliance failures
- Notify the Information Commissioners Office of any compliance failures that are material either in their own right or as part of a pattern of failures

The Martin Group takes compliance with this policy very seriously. Failure to comply places the Group and individuals at risk. Employees who fail to notify a breach or are found to have known or suspected a breach has occurred but not followed the correct reporting procedures may be subject to disciplinary proceedings.

16. Training and Awareness

Employees will receive suitable training on data protection law specific to their role. This will include training on UK GDPR, what constitutes a breach, how to identify a breach and how breaches should be reported. Employees must complete all training they are nominated to undertake. Employees who change roles or take on new responsibilities, will receive additional data protection training relevant to their new role or responsibilities.

17. Audits and Monitoring

Regular audits to manage and mitigate risks related to data protection will ensure the data register is maintained to include accurate, relevant data. The register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Data Controllers and Processors will conduct regular data audits as defined by the procedures contained in our Integrated Management Systems.

This policy is reviewed annually by the ISM/DPM. However, we have the right to change this policy at any time.
We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives. If you have any queries or concerns about Data Protection, please contact the ISM/DPM at data@hwmartin.com.

References

Policies, procedures and guidance within the ISMS should be read alongside this policy.

J. Clegg

James Clegg
Group Director HSEQ, Risk and Compliance