



## Data Protection and Privacy Policy

### Policy Statement

Johnston Vulcanising and Services Ltd. is committed to protecting the privacy and personal data of all employees, contractors, clients, and other stakeholders. This policy ensures compliance with UK data protection laws, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and outlines the procedures for safeguarding personal information.

### Scope

This policy applies to all employees, contractors, and operations within Johnston Vulcanising and Services Ltd., including those involved in quarrying, vulcanising activities, construction projects, sites, and offices in the UK.

### Responsibilities

- **Senior Management:** Ensure overall compliance with data protection regulations, provide necessary resources for data protection measures, and promote a culture of privacy and security.
- **Data Protection Officer (DPO):** Oversee the implementation and monitoring of data protection procedures, handle data protection inquiries, and provide training and guidance.
- **Managers and Supervisors:** Ensure staff follow data protection procedures, conduct regular inspections, and report any concerns or incidents.
- **All Employees and Contractors:** Comply with data protection procedures, report any issues, and participate in relevant training and awareness programs.

### Procedures

1. **Data Collection and Use**
  - Collect personal data only for legitimate business purposes and ensure it is relevant, accurate, and kept up-to-date.
  - Limit the collection of personal data to what is necessary for the purposes for which it is processed.
  - Use personal data only for the purposes for which it was collected, unless explicit consent is obtained for other uses.
2. **Data Storage and Security**
  - Store personal data securely, using appropriate technical and organizational measures to protect against unauthorized access, alteration, or destruction.
  - Implement access controls to ensure that only authorized personnel have access to personal data.
  - Regularly review and update security measures to address new and emerging threats.
3. **Data Retention and Disposal**



- Retain personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required by law.
  - Implement a data retention schedule to ensure data is not kept longer than necessary.
  - Ensure the secure disposal of personal data that is no longer needed, using methods such as shredding or secure digital deletion.
- 4. Data Subject Rights**
- Ensure individuals can exercise their rights under data protection laws, including the right to access, correct, delete, or restrict the processing of their personal data.
  - Provide clear and accessible information about how individuals can exercise their rights and respond to requests promptly and in accordance with legal requirements.
  - Maintain records of data subject requests and actions taken in response.
- 5. Data Breach Management**
- Implement procedures for identifying, reporting, and managing data breaches.
  - Notify the Information Commissioner's Office (ICO) and affected individuals of data breaches as required by law.
  - Conduct investigations into data breaches to determine the cause and implement corrective actions to prevent recurrence.
- 6. Training and Awareness**
- Provide training for all employees and contractors on data protection principles, legal requirements, and company procedures.
  - Include data protection training as part of the induction process for new employees.
  - Conduct regular refresher training and update employees on any changes to data protection laws or company policies.
- 7. Data Protection Impact Assessments (DPIAs)**
- Conduct DPIAs for any new or significantly changed processes that involve the processing of personal data to identify and mitigate privacy risks.
  - Document the outcomes of DPIAs and implement any necessary measures to address identified risks.
- 8. Third-Party Data Processing**
- Ensure that any third-party service providers that process personal data on behalf of Johnston Vulcanising and Services Ltd. comply with data protection laws and company policies.
  - Enter into data processing agreements with third parties to ensure the protection of personal data.
- 9. Monitoring and Review**
- Monitor compliance with data protection procedures through regular audits and inspections.
  - Review and update the data protection and privacy policy and procedures as necessary to reflect changes in legislation, industry standards, and company operations.
  - Incorporate feedback from employees, audits, and incidents into policy updates.



Johnston Vulcanising and Services Ltd. is dedicated to ensuring the protection of personal data and maintaining the privacy of all stakeholders. We expect all personnel to adhere to this policy and report any concerns promptly.

### Contact

For any questions or concerns about this policy, please contact Aaron Johnston by email at [Aaron@jvsuk.co.uk](mailto:Aaron@jvsuk.co.uk) or call 07495 376466.

Signed: A Johnston  
Date: 21/05/2025