

## Causeway Donseed Portal

### Introduction

Causeway Donseed is biometric verification software used to streamline staff time and attendance logging and reduces business risks across our sites. Employing biometric sign-in and sign-out software ensures consistent, reliable and accurate project data.

The benefits of using such systems include:

1. Accurate biometric Verification  
*Fingerprint and facial recognition enabled devices help us to reduce time theft and fraud and eliminate unreliable and slow paper-based processes.*
2. Reduce Administrative Costs  
*Automated attendance tracking reduces effort and increases efficiency and accuracy. Causeway Donseed helps us monitor budgeted vs. actual hours for a clear picture of actual hours worked on site.*
3. Designed for Construction Sites  
*Causeway Donseed has been designed with the industry in mind, to address the specific needs, challenges and use-cases of engineering and construction projects.*

### Policy

- All MIDA Civil Engineering sites, including Head Office, will have a Causeway Donseed device installed at the most convenient location on site.
- MIDA Operations Department will initially attend site and ensure all staff are set up correctly. A step-by-step guide has been provided to all sites on the signing-in and enrolment process which should be followed.
- It is all employees responsibility to be compliant and sign-in and sign-out on the Causeway Donseed device on each attendance at any MIDA Civil Engineering site. Failure to do so will result in the employee possibly being exempt from the company payroll until this is resolved. If the employee fails to sign-out more than once, this will delay payment.
- If an employee is attending more than one site in that given day, it is their responsibility to sign-in and sign-out of the sites to ensure our data displays correctly.
- All employees will have a QR code on their phone which they will scan on the device on sign-in. As a back-up, fingerprint recognition will be used, but only as a second option. As a company, we want the process to be as efficient as possible, and this is the reason we have set-up this new process using a QR code log-in, as we believe it will allow for a much smoother sign-in and sign-out process.
- It is the employee's responsibility to report any issues with signing-in or signing-out of the Causeway Donseed device to their Site Manager at the earliest opportunity, who must report this into the Operations Department, who will deal with the issue and resolve accordingly.
- Employee data is held in accordance with GDPR compliance.

## Causeway SkillGuard

### Introduction

Causeway SkillGuard is a digital passport that keeps track of our workforce's skills, competencies, experience, training and more. The solution allows us to validate authority to work and ensure our teams meet the requirements of the project or site that they're working on.

The benefits of using the Causeway SkillGuard system include:

1. **Manage team members**  
*Ensures our whole site team is fully qualified and onboarded. Allows us to assign jobs based on the best skills match, and manage risk, safety and compliance.*
2. **Enhance project visibility**  
*Allows us to manage and optimise resources and respond quickly to changes in scope with real-time worker data. Creates an audit trail, minimises risk exposure and increases efficiency.*
3. **Streamline site operations**  
*Improves our on-site processes and automates administrative tasks to increase efficiency allowing us to manage large teams.*
4. **Improved communication**  
*Built in communication functions allows us to send alerts and messages to teams and individuals, facilitating agile working.*

## Biometric Data Collection and Use

1. **Definition of Biometric Data**  
Biometric data refers to unique physical characteristics used for identification purposes, such as fingerprints, facial recognition, or iris scans, collected through biometric scanning devices at designated signing-in locations.
2. **Purpose of Biometric Data**  
The biometric data collected will be used solely for the purpose of confirming the identity of individuals during the signing-in process. It will serve as a secure and efficient alternative to traditional methods of sign-in, such as badges or passwords.
3. **Types of Biometric Data Collected**
  - Fingerprint scanning
  - Facial recognition (if applicable)
  - Other biometric identifiers as deemed necessary
4. **Consent**  
Individuals will be required to provide explicit consent to the collection and use of their biometric data before the process begins. This consent will be documented and recorded electronically.

## 5. Data Security and Privacy

- Biometric data will be stored in a secure database with encryption to prevent unauthorised access.
- Only authorised personnel will have access to biometric data, and access will be strictly limited to the purpose of verifying identity for sign-in purposes.
- Biometric data will not be shared with third parties except as required by law or in accordance with this policy.

## 6. Data Retention

Biometric data will be retained only for the duration of employment or authorised access. Once an individual's access rights have been revoked or terminated, their biometric data will be deleted from the system within a reasonable timeframe.

## 7. User Rights

- Individuals have the right to access their biometric data upon request.
- Individuals may opt out of the biometric sign-in system by using an alternative sign-in method if available.
- In cases where individuals wish to revoke consent, they can request to be removed from the biometric system, but alternative methods for sign-in will need to be arranged.

## 8. Compliance with Legal Requirements

The collection, use, and storage of biometric data will be in compliance with applicable data protection laws and regulations, including but not limited to:

- The United Kingdom *General Data Protection Regulation (GDPR)*
- Local privacy and biometric data protection laws

## Responsibilities

### 1. Management Responsibilities

- Ensure the implementation of this policy and that biometric systems are functioning properly.
- Provide training to staff on the ethical and legal use of biometric data.
- Regularly review the biometric data storage and retention practices to ensure compliance with this *policy*.

### 2. Employee Responsibilities

- Consent to the collection and use of biometric data as per this policy.
- Notify management if they have concerns regarding their biometric data or the sign-in process.
- Use the biometric sign-in system as intended and report any issues promptly.

### 3. Vendor Responsibilities

- Ensure that any third-party biometric systems are compliant with this *policy* and applicable data protection laws.
- Assist in securing biometric data and maintaining data integrity.

## System Access and Monitoring

- Biometric systems will be monitored regularly for unauthorised access or malfunctions.
- Any attempt to bypass or manipulate the biometric system will be treated as a violation of company policy and subject to disciplinary action.

## Exceptions

- In case of system failure, manual sign-in procedures will be available as a backup, with proper identification verification.
- Individuals with disabilities or special needs may request accommodations and be provided alternative sign-in methods.

## Policy Violations

Any violation of this policy, including unauthorised access to biometric data, tampering with the biometric system, or failure to comply with the consent and security procedures, will result in disciplinary actions, including potential termination of access rights or employment.

## Policy Review and Updates

This policy will be reviewed annually to ensure compliance with applicable laws and regulations and to address any changes in the organisation's biometric sign-in practices.

**Signed:**



**Date:** 23<sup>rd</sup> February 2026

James Brown

Regional Managing Director