Data Protection and Security Policy

ECMS Services Ltd (ECMS) is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) and Data protection.

The company will strive to follow procedures closely which aim to ensure that all employees, contractors, partners, or others who have access to any personal data held by or on behalf of are fully aware of and abide by their duties under the General Data Protection Regulation (GDPR)

In order to operate efficiently, ECMS has a need to collect and use information about people with whom it works. These include current, past, and prospective employees, clients, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded, and used, and whether it is:

- **On paper**
- **In computer records**
- **Via e-mail**
- **Recorded by any other means**

At ECMS we regard the lawful and correct treatment of personal information as very important to our successful operations and to maintaining confidence between us and our clients.
We will ensure that we treat personal information lawfully and correctly.
We will protect data from unauthorised access, alteration or destruction.
We will ensure data is up to date and accurate

ECMS will inform users of their rights under GDPR, how we plan to use the user's data and provide users with a way to contact us if they have any questions or concerns about their data.

ECMS will communicate this policy and make sure that all employees are aware of it. Employees are trained on how to protect data and what to do if they suspect that it has been compromised.

On Paper

All confidential paper waste is shredded in the office before it is disposed of and CCTV cameras operate on the premises of our office

On Our Computer Records

All computers in the ECMS office have a firewall and virus-checking software installed; this will prevent any loss of data stored on the systems. The operating system is set up to receive automatic updates. Personnel in the office have access to only the information they need to do their specific job. We also have an anti-spyware tool installed onto each computer. This prevents fraudsters from capturing important data such as passwords, banking credentials and credit card details.

ECMS take regular back-ups of the information on our server which are kept in a separate place to prevent loss of information if computers were to fail.

Data sent via email

ECMS try not to send any e-mails with content that could cause harm if lost or misused. However, when this is unavoidable, we make certain that the e-mail is sent to the right person and no-one else. When sending an email to a recipient who does not want their address revealed to other recipients, we use the blind carbon copy (bcc) icon.

Other security means

Windows and doors are always locked at the end of the day with no information left on display.

Security within the site location

ECMS make an effort to employ trusted staffs. Before staff commence work on site, we make sure to collect from them a valid form of identification, check for rights to work in the UK, age restrictions and other such lawful requirements.

Although not all staff have a DBS check, the trait is considered desirable throughout the process of employing staff, and it is our policy to carry out any DBS checks requested by the client. Any member of staff working in an environment where there may be younger or vulnerable people ECMS will ensure a DBS check is completed and records are held at our Head Office site.
This enables us to make safer recruitment decisions, identifying candidates who may be more suitable to be put in a trusted position. They are educated against listening to and disclosing confidential information discussed within the sites we facilitate and reminded the importance of the locking of doors and the confidentiality of and unlock codes/keys. If necessary, or obliged to by the client, staff wear a security badge on site.

James Grimsley
Director

Date: 08/01/2025
Review: January 2026