CS2 Transport Ltd – Data Protection Policy.

Introduction.

CS2 Transport Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handles and stored to meet the company's data protection standards and to comply with the law.

Why this policy exists.

This data protection policy ensures that CS2 Transport Ltd:

-Complies with the data protection law (GDPR) and follows good practice

-Protects the rights of relevant individuals and companies

-Is open about how it stores and processes individuals' data

-Protects itself from the risk of data breach.

Data protection law.

The Data Protection Act 1998 describes how open organisations must collect, handle and store personal information. These rules must apply regardless of whether the data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored and not disclosed unlawfully. The data protection act is underpinned by eight importation principles; these say that personal data must:

-Be processed fairly and lawfully.

-Be obtained only for specific, lawful purposes.

-Be adequate, relevant and not excessive.

-Be accurate and kept up to date.

-Not be held any longer than necessary.

-Processed in accordance with the rights of data subjects.

-Be protected in appropriate ways.

-Not be transferred outside of the European economic area, unless that country or territory also ensures adequate level of protection.

People, risks and responsibilities.

This policy applies to:

-All staff at CS2 Transport Ltd.

-All contractors, customers and suppliers of CS2 Transport Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the data protection act 1998. This can include:

-Names of individuals.

-Postal addresses.

-Email addresses.

-Telephone numbers.

-Any other information relating to individuals.

Data protection risks.

This policy helps protect CS2 Transport Ltd from some very real data security risk, including:

-Breaches of confidentiality. For instance, information given out inappropriately.

-Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

-Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities.

Everyone who works for CS2 Transport Ltd has some responsibility for ensuring data is collected, stored and handles appropriately. Each person that handles personal data must ensure that it is handles and processed in line with this policy and data protection principles.

-CS2 Transport Ltd Directors are ultimately responsible for ensuring that CS2 Transport Ltd meet their legal obligations.

The company's Directors will implement a management system to address and manage their obligations in relation to:

-Keeping the business updated about data protection responsibilities, risks and issues.

-Reviewing all data protection procedures and related policies, in line with an agreed schedule.

-Arranging data protection training and advice for people covered by this policy.

-Handling data protection questions from staff and anyone else covered in this policy.

-Dealing with requests from individuals to see the data CS2 Transport Ltd holds about them.

-Checking and approving any contracts or agreements with third parties that may handle the company sensitive data.

-Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

-Performing regular checks and scans to ensure that security hardware and software is functioning properly.

-Evaluating any data for third party services that the company is considering using to store and process data.

-Approving all data protection statements attached to communications such as emails and letters addressing any data protection queries from journalists and media outlets like newspapers.

-Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- Any information received via the companies Whistleblowing Policy (a copy of which is available on request) will be treated in the same confidential terms and conditions.

General staff guidelines.

-The only people able to access data covered by this policy should be those who need it for business use.

-Data should not be shared informally.

-When access to confidential information is required, employees to help them understand their responsibilities when handling data.

-Employees should keep all data secure by taking sensible precautions and following the guidelines below. In particular, strong passwords must be used and they should never be shared.

-Personal data should not be disclosed to unauthorised people, either within the company or externally.

-Data should be reviewed regularly and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of. Employees should request help from their line manager if they are unsure about any aspect of data protection.

Data Storage.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Operations Director

-When data is stored on paper, it should be kept in a secure place where unauthorised people could see them, such as a printer.

-Data printouts should be shredded and disposed of securely when no longer required.

-When data is stored electronically, it should be protected from unauthorised access, accidental deletion and malicious hacking attempts.

-Data should be protected by strong passwords and never shared between employees.

-If data is stored on removable media such as a USB, these should be kept locked away securely when not being used.

-Data should only be stored on designated drivers and servers and should not be uploaded to any on approved computing services.

-Servers containing personal data should be cited in a secure location, away from general office space.

-Data should be backed up frequently. Those backups should be tested regularly in line with company standard back up procedures.

-Data should never be saved directly to laptops or other mobile devices such as tablets or phones.

-All servers and computers containing data should be protected by approved security software and a firewall.

Data Use.

Personal data is of no value to CS2 Transport Ltd unless the business can make use of it. However, it is when personal data is accessed and used to be at the greatest risk of loss, corruption or theft:

-When working with personal data, employees should ensure that the screens of their computers are always locked when left unattended.

-Personal data should not be shared informally. In particular care must be taken when sending/receiving personal data via email.

-Personal data should never be transferred outside the European economic area.

-Employees should not save copies of their personal data to their own computers.

Data accuracy

-The law requires CS2 Transport Ltd to take reasonable steps to ensure that data is kept accurately and up to date.

-It is the responsibility of all employees who work with data to take reasonable steps to ensure that data is accurate and up to date as possible.

-Data will be held in as fewer places as necessary.

-Staff should not create any unnecessary additional data sets.

-Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

-CS2 Transport Ltd will make it easy for data subjects to update their information.

-Data should be updated as inaccuracies are discovered. From instance, if a customer could no longer be reached on their stored telephone number, it should be removed from the database.

Subject access request.

All individuals who are the subject of personal data held by CS2 Transport Ltd are entitled to:

-Ask what information the company hold about them and why.

-Ask how to gain access to it.

-Be informed how to keep it up-to-date.

-Be informed how the company is meeting its data protection obligations.

-If an individual contacts the company requesting this information, this is called a subject access request. Subject access request from individuals should be made by email, addressed to Alex Elliott at alex@cs-2.co.uk. The company aim to provide the relevant data within 14 days. CS2 Transport Ltd will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons.

The Data Protection Act allows personal data to be disclosed to law-enforcement agencies without the consent of the data subject. Under these circumstances, CS2 Transport Ltd will disclose the

requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the companies' legal advisers when necessary.

Providing information.

CS2 Transport Ltd aims to ensure that the individuals are aware that the data is being processed, and that they understand:

-How the data is being used.

-How to exercise that right.

To these ends, the company has a privacy statement, setting out how data relating to the individuals is used by the company. This is available on request.

Signed …… **Gary Turney Managing Director**

Date ……