Corporate Potential Ltd Data Protection Policy

Key Details

Policy prepared by:	Practice Manager
Approved by Director:	Lisa Wynn
Policy became Operational:	3rd November 2006
Next Review Date:	3rd November 2019

Introduction

Corporate Potential Ltd needs to gather information about individuals.

These can include customers, suppliers, business contacts, employees & sub-contractors and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled, stored and subsequently destroyed to meet the company's data protection standards, and to comply with the law.

Why this Policy Exists

This data protection policy ensures Corporate Potential Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of staff customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations, including Corporate Potential Ltd must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles, these say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection.

People, Risks & Responsibilities

Policy Scope

This policy applies to:

- The Head office of Corporate Potential Ltd
- All branches of Corporate Potential Ltd
- All staff, volunteers and sub-contractors of Corporate Potential Ltd
- All contractors and sub-contractors, suppliers and other people working on behalf of Corporate Potential 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
- Contact telephone numbers
- Date of Birth
- Copy of Passport
- Plus any other information relating to individuals

Data Protection Risks

This policy helps to protect Corporate Potential Ltd from some very real data security risks, including:

- Breaches of confidentiality. For instance information being 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 or is sub-contracted by Corporate Potential Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility;

- The Director of Corporate Potential Ltd is ultimately responsible for ensuring that it meets its legal obligations

- Data Protection Officers: The Operations team are responsible for:
    - Keeping the Director 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 the people covered by this policy.
    - Handling data protection questions covered by this policy.
    - Dealing with requests from individuals to see the data Corporate Potential Ltd holds about them (also called subject access requests).
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- IT: All sub-contractors are responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the company is considering using to store or process data. For instance cloud computing services.

- Marketing: All sub-contractors are responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries form journalists or media outlets.
  - Where necessary, ensuring marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those that need it to complete their task.
- Data should not be shared informally. When access to confidential information is required, this can be requested from those that control it.
- Corporate Potential Ltd will provide training to all relevant sub-contractors to help them understand their responsibilities when handling data.
- Data should be kept 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 regularly reviewed and updated if it is found to be out of date. If it is no longer required, it should be deleted and disposed of.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or the data controller.

When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- No paper or printouts should be left where authorised people can see them.
- Data printouts should be shredded and disposed of securely when no longer required.

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

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (CD, DVD) these be kept securely locked away when not in use.
- Data should only be stored on designated drivers and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software.

Data Use

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

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Personal data should not be transferred outside of the European Economic Area unless that country or territory also ensures an adequate level of protection.

Data Accuracy

The law requires Corporate Potential Ltd to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Corporate Potential Ltd should put into ensuring its accuracy.

It is the responsibility of all sub-contractors that work with data to take reasonable steps to ensure it is kept as accurate and as up to date as possible.

- Data will be held in as few places as necessary. No unnecessary additional data sets should be created.
- All sub-contractors that work with data should take every opportunity to ensure data is updated.
- Corporate Potential Ltd will make it easy for data subjects to update the information Corporate Potential Ltd holds about them.
- Data should be updated as inaccuracies are discovered.
- Marketing databases should be updated regularly.

Subject Access Requirements

All individuals who are the subject of personal data held by Corporate Potential Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- 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 requests from individuals should be made by email, address to the data controller (dataprotection@corporatepotential.com).

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Corporate Potential Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the senior partners and legal advisors where deemed necessary.

Providing Information

Corporate Potential Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

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

This is available upon request and a version of this is available on the company website; www.corporatepotential.com