



McCarthy's  
Inspiring Spaces....



DESIGN



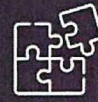
BUILD



INTERIORS



MOTOR RETAIL



FRAMEWORK



HEALTH & SAFETY  
AND ENVIRONMENTAL



# DATA PROTECTION POLICY

Systems House, Broad Lane, Coventry CV5 7AX  
t: 024 7646 8866 e: [sales@mccarthygroup.co.uk](mailto:sales@mccarthygroup.co.uk)  
[www.mccarthygroup.co.uk](http://www.mccarthygroup.co.uk)

Managing Director: S R McCarthy BSc (Hons), Chairman: B McCarthy.  
Company Registration No. 1692577. McCarthy Associates Ltd trading as McCarthy's.





**McCarthy's**  
Inspiring Spaces....



DESIGN



BUILD



INTERIORS



MOTOR RETAIL



FRAMEWORK



HEALTH & SAFETY  
AND ENVIRONMENTAL



## INTRODUCTION

**McCarthy's** is a company specialising in refurbishment, space planning and corporate relocation and professional safety services. We pride ourselves on our concept to completion approach incorporating Build, Interiors, Furniture and Environment.

**McCarthy's** needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, 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, handled and stored to meet the company's data protection standards — and to comply with the law.

This data protection policy ensures McCarthy's:

- Complies with data protection law and follow 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 McCarthy's, 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 which state 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



McCarthy's  
Inspiring Spaces....



DESIGN



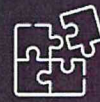
BUILD



INTERIORS



MOTOR RETAIL



FRAMEWORK



HEALTH & SAFETY  
AND ENVIRONMENTAL



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

### **POLICY SCOPE**

This policy applies to:

- The head office of McCarthy's
- All Staff, Sub- contractors, suppliers and other people working on behalf of McCarthy's

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
- ...plus any other information relating to individuals

### **DATA PROTECTION RISKS**

This policy helps to protect McCarthy's 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.





DESIGN



BUILD



INTERIORS



MOTOR RETAIL



FRAMEWORK



HEALTH & SAFETY  
AND ENVIRONMENTAL



## RESPONSIBILITIES

Everyone who works for or with McCarthy's 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 **board of directors** is ultimately responsible for ensuring that McCarthy's meets its legal obligations, including;

- Addressing any data protection queries from journalists or media outlets like newspapers.

The **data protection officer** is responsible for:

- Keeping the board 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 from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data McCarthy's 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.
- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

The **IT manager** is 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.



DESIGN



BUILD



INTERIORS



MOTOR RETAIL



FRAMEWORK



HEALTH & SAFETY  
AND ENVIRONMENTAL



## GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **McCarthy's will provide training** to all 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 **regularly reviewed 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 or the data protection officer 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 IT manager. 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.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- 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 and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an 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.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones – all smart phones will employ a 30second lock.





DESIGN



BUILD



INTERIORS



MOTOR RETAIL



FRAMEWORK



HEALTH & SAFETY  
AND ENVIRONMENTAL



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

## **DATA USE**

When personal data is accessed and used 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. In particular, it should never be sent by email, as this form of communication is not secure. Where data has to be transferred by e-mail, it shall be encrypted.
- Personal data should never be transferred outside of the European Economic Area.

## **DATA ACCURACY**

The law requires McCarthy's to take reasonable steps to ensure data is kept accurate and up to date.

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

- Data will be held in as few 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.
- McCarthy's will make it easy for data subjects to update the information McCarthy's hold about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should either be updated or removed from the database.

## **SUBJECT ACCESS REQUESTS & THE PROVISION OF INFORMATION**

All individuals who are the subject of personal data held by McCarthy's are entitled to:

- Ask what information the company holds 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 requests from individuals should be made by email, addressed to the data controller at



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, McCarthy's will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

### **COMMUNICATION & REVIEW**

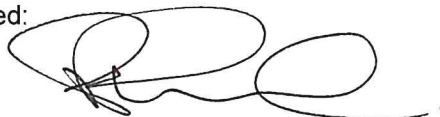
We will communicate this policy to all our employees and ensure that they are given appropriate training to raise awareness of GDPR issues.

McCarthy's will review this policy on an annual basis, taking account of any changes within legislation, our organization and other factors.

Any changes to our policy will be communicated to our employees via our electronic management system and through additional tool box talks if applicable.

McCarthy's will make this policy available, when requested, to interested parties including members of the public.

Signed:



Steve McCarthy  
Managing Director

Last Review Date: 06 January 2023

Amended Date:

Reviewed Annually

