Data Protection Policy

Introduction

CATCH needs to gather and use certain information about individuals.

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

The policy describes how the personal data must be collected, handled, 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 CATCH:

- 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 2018 describes organisations, including CATCH – 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.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Policy scope

This policy applies to:

- All employees of CATCH/apprentices
- All associates, contractors, suppliers, and other people working on behalf of CATCH

It applies to all data the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Financial information
- Plus, any other information relating to individuals

Data protections risks

This policy helps to protect CATCH from some very real 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 with CATCH has some responsibility for ensuring data is collected, stored, and handled appropriately. Each member of staff 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** are ultimately responsible for ensuring that CATCH meets its legal obligations
The **CEO/COO** is responsible for:

- Keeping the board updated about data protection responsibilities, risks, and issues
- Approve all data protection procedures and related policies in line with an agreed schedule.
- Approving any data protection statements attached to communications such as emails and letters

The **HR department** are responsible for:

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

General staff guidelines

- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meets acceptable security standards
- Data should not be shared informally. When access to information contained within their personnel file is required, employees can request it from their line manager.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used
- 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.
- 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, e.g. on a printer
- Data printouts should be shredded and disposed of securely when no longer required
- If data is stored on removable media, these should be kept locked away securely when not being used
- 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.
- All servers and computers containing data should be protected by approved security software and a firewall

Providing information

CATCH aims to ensure that individuals are aware that their data is being processed and 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 individuals is used by the company.

This is available on request. A version of the statement is also available on the company's website.

We are committed to reviewing this policy.

Signed: James McIntosh
James McIntosh (Jul 25, 2023 15:25 GMT+1)

James McIntosh

Director of Skills/COO

Date: 25/07/23