# H Charlesworth & Co Ltd

## data protection policy

## context & overview

### key details

| | |
|---|---|
| • Policy prepared by: | Richard Pearson |
| • Approved by board / management on: | 29th May 2018 |
| • Policy became operational on: | 29th May 2018 |
| • Next review date: | 29th May 2021 |

| | |
|---|---|
| Information Commissioners Office (ICO) | Reg No: Z6088402 |
| Contact details for the ICO: | https://ico.org.uk |
| Visit the ICO website or call | 0303 123 1113 |

## Introduction

H Charlesworth & Co Ltd (trading as Charlesworth Press) and Hammonds (a trading division of H Charlesworth & Co Ltd) need to gather and use certain information about individuals. We treat personal data and private information with the respect it deserves and have never and will never sell or transfer any data to any person or company outside of our business for use in any other way unless directly requested to do so by the Data Controller (our Customer).

These can include customers, suppliers, business contacts, employees and other people the organization 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, General Data Protection Regulation (GDPR) – and to comply with the law.

Within this document will be instructions on what to do and how to inform both management and professional bodies of any data breach.

## why this policy exists

The data protection policy ensures H Charlesworth & Co Ltd:

- 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 H Charlesworth & Co – 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:

- 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 for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

## people, risks and responsibilities

### policy scope

This policy applies to:

- H Charlesworth & Co Ltd. Company No. 1143652
- All staff and volunteers of H Charlesworth & Co Ltd
- All contractors, suppliers and other people working on behalf of H Charlesworth & Co 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 to protect H Charlesworth & Co 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 with H Charlesworth & Co Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

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

These individual people have key areas of responsibility:

- Group Director, Mark Gray is ultimately responsible for ensuring that H Charlesworth & Co Ltd meets its legal obligations and when necessary Mark Gray is also
    - responsible for reporting to the Information Commissioners Office for further third party investigation.

- IT Manager, Richard Pearson 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 storage or FTP storage.

The Finance Manager, Nicola Empson is responsible for:

- Ensuring all company sensitive data is treated as such and stored in the correct manner in locked cupboards.
- Safeguarding customer details to the best of your ability within software such as Sage and Tharstern. This means keeping password protections current and only giving password access to those that require it to carry out their role within the business.
- Ensuring all staff details including but not exhaustive of:
    - Staff addresses
    - Staff telephone numbers
    - Staff bank account details
    - Staff contracts and terms of employments
    - Any other sensitive data that can be linked to an individual staff member.
- Ensuring data sensitive orders are treated with the upmost confidentiality.
- Reporting any data breach to Richard Pearson for further investigation.
- When data sensitive orders are being throughput they should ensure no persons other than those named within this policy are within close proximity to cause data breach other than those approved by Richard Pearson. Instances such as an approved contractor that has been briefed on this policy would constitute an exception.

## 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.
- H Charlesworth & Co Ltd 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 with any persons outside of the company.
- Personal data should not be disclosed to unauthorized 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 managers, supervisors 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 Richard Pearson.

- 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 or desk.
- 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 outside of the company.
- If data is stored on removable media (like a USB drive or CD), these should be kept locked away securely in the safe within the meeting room when not in use.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- 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 servers and computers containing data should be protected by approved security software and firewalls.

## data use

Personal data is of no value to H Charlesworth & Co 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. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data should never be transferred outside of the European Economic Area.

## data accuracy

The law requires H Charlesworth & Co Ltd 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 H Charlesworth & Co Ltd should put into ensuring its accuracy.

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 unnecessary additional data sets/copies.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customers' details when they call.
- H Charlesworth & Co Ltd will make it easy for data subjects to update the information H Charlesworth & Co Ltd holds 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 be removed from the database.
- It is Sales Directors (Gary Wild) responsibility to ensure marketing databases and company databases are kept up to date as often as possible as changes become apparent or the company is made aware of such amendments.

## subject access requests

All individuals who are the subject of personal data held by H Charlesworth & Co Ltd 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 IT Manager at subjectaccessrequests@charlesworth.com .

Individuals will be charged £10 per subject access request. H Charlesworth & Co Ltd will aim to provide the relevant data within 14 days.

H Charlesworth & Co Ltd 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, H Charlesworth & Co Ltd will disclose requested data. However, H Charlesworth & Co Ltd will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

## providing information

H Charlesworth & Co 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 will always respond quickly to any request for information and will always operate within this policy and the rules here in set out.

## audit of data processing

H Charlesworth & Co Ltd will hold a record within this policy folder to track all data processing requests.

This is compulsory and must be kept up to date for every order that requires any element of data processing.

This will raise the awareness within the team at the time of the order and will track each and every time we process any data whether that be on a customer's request or for our own use.

## file retention

Files will only be held on machines that are secured by firewalls and virus detection software. These files must only be stored whilst the job is being processed. On completion of the job this data must be removed from the system and the individual operator must ensure no trace is left within their machine such as recent histories and recycle bins.

Whilst files are stored during order process no machine is to be left unattended without being locked with a user password and secured within an encrypted folder. Richard Pearson will advise of any procedure that any operator is unsure of.

H Charlesworth & Co Ltd will only ever use data supplied by a customer for the purpose it is intended and will always only deal as a processer not a controller for such data. With that in mind the company will never use this data for any other purpose and will destroy the data after use. Any request from the customer to store such information will be rejected on the grounds of Data Protection and GDPR Regulations.