Murray & Henderson
CHARTERED ACCOUNTANTS

Privacy, Data protection & GDPR policy

Context and overview

Key details

- • Policy prepared by: **Michael Reynolds**
- • Approved by Owner on: 24th May 2018
- • Policy became operational on: 25th May 2018
- • Next review date: 25th April 2019

Introduction

Murray and Henderson Chartered Accountants 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.

As such, Murray and Henderson Chartered Accountants, is registered with ICO (Information Commissioner's Office) as both data controllers & processors. Our Policy Registration Document and our "Statement Of Registration Entry" can be found on the ICO website at https://ico.org.uk/esdwebpages/search with ref: Z8813697

This policy describes how this personal data and other non-personal data, must be collected, handled and stored to meet the company's data protection standards which adhere to both GDPR and the Data Protection Act 1998

Murray and Henderson Chartered Accountants, as a Chartered Accountancy service, acts as both controller and processor of data, and is bound by GDPR, Data Protection laws, and ethics.

Why this policy exists

This data protection policy ensures Murray and Henderson Chartered Accountants:
• Complies with data protection law, The Data Protection Act 1998 and follows good practice
• Complies with GDPR (*General Data Protection Regulation*)
• 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

Murray & Henderson
CHARTERED ACCOUNTANTS

GDPR & Data protection law

The Data Protection Act 1998, and General Data Protection Regulation April 2016 describes how organisations — including Murray and Henderson Chartered Accountants— must collect, handle and store personal information and other non-personal sensitive data.
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 & GDPR is underpinned by important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be obtained and used with specific consent
4. Be adequate, relevant and not excessive
5. Be accurate and kept up to date
6. Not be held for any longer than necessary
7. Processed in accordance with the rights of data subjects
8. Be protected in appropriate ways
9. 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:

• The head office of Murray and Henderson Chartered Accountants
• All branches of Murray and Henderson Chartered Accountants
• All staff and volunteers of Murray and Henderson Chartered Accountants
• All contractors, suppliers and other people working on behalf of Murray and Henderson Chartered Accountants

It applies to all data that the company holds and/or processes, relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998.
This can include:

- personal details including Names of individuals
- family, lifestyle and social circumstances
- goods and services
- financial details
- education details
- employment details
- Postal addresses

- Email addresses
- Telephone numbers
- Contact Full Name,
- Company,
- Business Telephone Number,
- Business Email Address,
- Job Title,
- Job Function and Responsibilities
- Financial Information supplied by clients for processing

We also process sensitive classes of information that may include:

- physical or mental health details
- Nationality
- Country Of Residency
- trade union membership

Who the information is processed about

We process personal information about customers and clients, advisers and other professional experts and employees.

We also process data on behalf of clients or customers, therefore we are not technically the controller of that data, but act as the processor, thus we provide this function on the understanding the controller (usually the client or customer) has abided by Law in terms of Privacy, Data Protection and GDPR.

Data protection risks

This policy helps to protect Murray and Henderson Chartered Accountants 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, unless it is for legitimate purpose specific to a lawful and necessary task.

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

Responsibilities

Everyone who works for or with Murray and Henderson Chartered Accountants has some responsibility for ensuring data is collected, stored and handled and protected 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 **Company Owner** is ultimately responsible for ensuring that Murray and Henderson Chartered Accountants meets its legal obligations.

• The **[data protection officer], [Michael Reynolds],** is responsible for:

- Keeping the Company Owner 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 Murray and Henderson Chartered Accountants 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.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

• The **[IT Company], [Ensite Business Technology Ltd],** 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.

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 senior staff.

• **Murray and Henderson Chartered Accountants 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 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 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**.

• Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

• An **up to date record** of what kinds of data is stored and where by the Data Protection Officer.

• **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 only shared between employees who have the required access needs..

• If data is **stored on removable media** (like a USB memory device or DVD), these should be kept locked away securely when not being used.

• Data should only be stored on **designated drives**, and should only be uploaded to an **approved cloud computing services**.

• Computers containing personal data should be **sited in a secure location**, away from general public access.

• Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

• All computers containing data should be protected by ESET Endpoint Antivirus **approved security software and MS Windows firewall**.

Murray & Henderson
CHARTERED ACCOUNTANTS

Electronic Data use

Personal data is of no value to Murray and Henderson Chartered Accountants 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, unless fully encrypted and only via PCs that have the necessary encryption software to accomplish this.

• Data must be **encrypted before being transferred electronically**. The IT company can explain how to send data to authorised external contacts.

• Personal data should **never be transferred outside of the European Economic Area**, unless fully encrypted and the receiving 3rd party vendor complies with all aspects of Data Protection and GDPR

• Employees **should not save copies of personal data to their own computers,** unless on a designated drive/folder for that specific purpose. Always access and update the central copy of any data when applicable.

Marketing

Murray and Henderson Chartered Accountants do not engage in any direct marketing, and communication via electronic (e.g. email). Telephone, or Traditional Postal Mail, is strictly limited to "Legitimate Purpose" in order to provide the Client or Customer with a service in their direct interest, or because it is necessary to complete the service requested.
In order to do this, we comply with the GDPR statements produced by ICO on these matters and abide with the following "Best Practices" checklist.

.

☐ We have checked that legitimate interests is the most appropriate basis.
☐ We understand our responsibility to protect the individual's interests.
☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
☐ We have identified the relevant legitimate interests.
☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
☐ We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
☐ If we process children's data, we take extra care to make sure we protect their interests.
☐ We have considered safeguards to reduce the impact where possible.
☐ We have considered whether we can offer an opt out.
☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
☐ We keep our LIA under review, and repeat it if circumstances change.
☐ We include information about our legitimate interests in our privacy information.

Who the information may be shared with

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA) and GDPR (*General Data Protection Regulation*). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons, but only specific data as required, and will be what is judged as minimal data to complete the function.

Where necessary or required we share information with:

- business associates, professional advisers
- family, associates and representatives of the person whose personal data we are processing
- suppliers
- local and central government
- financial organisations
- ombudsmen and regulatory authorities
- credit reference and debt collection agencies
- healthcare professionals, social and welfare organisations
- current, past or prospective employers
- examining bodies
- service providers

Data accuracy

The law requires Murray and Henderson Chartered Accountants 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 Murray and Henderson Chartered Accountants 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 any unnecessary additional data sets.

Murray & Henderson
CHARTERED ACCOUNTANTS

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

• Murray and Henderson Chartered Accountants will make it **easy for data subjects to update the information** Murray and Henderson Chartered Accountants holds about them. For instance, via the company website.

• 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.

Employee Personal Data

The law requires Murray and Henderson Chartered Accountants hold specific personal data regarding our employees and share it with the required Government Bodies. This data will be held for the required minimum period when a person leaves the company.

Murray and Henderson Chartered Accountants may also hold other data required for internal use, such as performance, training, qualifications etc., and will be accessible only by senior staff responsible for the management of the employees.

Subject access requests

All individuals who are the subject of personal data held by Murray and Henderson Chartered Accountants 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 enquiries@murrayhenderson.co.uk or made by standard postal mail to the data controller at our head office as listed on our website at http://murrayhenderson.co.uk/

The data controller can supply a standard request form, although individuals do not have to use this.

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.

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