GDPR Statement

Data Protection Act 2018 and the General Data Protection Regulation ((EU) 2016/679 (“GDPR”)

SEQOHS
Safe Effective Quality Occupational Health Service

bsi
UKAS MANAGEMENT SYSTEMS
0003
ISO 9001 2015 FS 557227

Commitment to social enterprise

Introduction

MOHS Workplace Health (MOHS) is required 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 is 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 MOHS:

- 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 describes how organisations – including MOHS – must collect, handle and store personal information of individuals.

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:

- 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
- be processed in accordance with the rights of data subjects
- be protected in appropriate ways
- not to 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:

- all employees of MOHS
- all service users
- all service providers

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 2018. This can include:

- names of individuals
- postal addresses
- email addresses
- telephone numbers
- organisation name
- unique reference numbers such as: national insurance number or clock number
- date of birth
- medical history

Data protection risks

This policy helps protect MOHS from rare data security risks, including:

- breaches of confidentiality eg, information being given out inappropriately
- failing to offer choice eg, all individuals should be free to choose how the company uses the data relating to them
- reputational damage eg, the company could suffer if hackers successfully gain access to sensitive data

Responsibilities

Everyone who works for or with MOHS has a 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, the following have key areas of responsibility:

MOHS board of directors: who are ultimately responsible for ensuring MOHS meets its legal obligations.

Data protection officer, Helen Hooper, chief executive, is responsible for:

- keeping the board updated about data protection responsibilities, risks and issues
- reviewing all data protection and related policies, in line with an agreed schedule
- handling data protection questions from employees; and anyone else covered by this policy
- dealing with requests from individuals to see the data MOHS holds about them, also known as 'Subject Access Request'
- checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

MOHS's IT support: ICM (Intuitive Computer Management) Is responsible for:

- ensuring all IT systems, services and equipment used for storage data meet required security standards
- performing monthly checks and scans to ensure security hardware and software is functioning properly
- evaluating any third party services MOHS is considering using to store or process data eg, cloud computing

MOHS's Digital Marketing Executive is responsible for:

- approving any data protection statements attached to communications such as emails and letters
- addressing any data protection queries from journalists or media outlets

- working with other staff, where necessary, to ensure marketing initiatives abide by the data protection principles

General staff guidelines

The only people able to access data covered by this policy is restricted to those who have a genuine need in line with their job role.

Data should not be shared informally.

MOHS will provide training to all employees to help them understand their responsibilities when handling data.

Employees will keep all data secure by taking sensible precautions and following the guidelines below:

- passwords will be strong and never shared
- personal data will not be disclosed to unauthorised people, either in the company or externally
- data will be regularly reviewed and updated if found to be out of date. If no longer required, it will be deleted
- employees will be encouraged to 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 data controller.

Stored data will be kept in a secure place, where unauthorised people cannot see or access 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 (and any files) will be kept in a drawer of filing cabinet in a locked room, with only relevant MOHS employees having access
- MOHS employees will ensure that paper and printouts are not left where unauthorised people can see them, eg on a printer
- data printouts will be shredded and disposed of securely when no longer required. Shredding is removed from the building by an accredited body in sealed sacks, taken to the site of the shredding in a triple locked vehicle and placed straight from the van into the shredder.

Electronically stored data will be protected from unauthorised access, accidental deletion or malicious hacking attempts:

- data is protected by strong passwords that are never shared between employees
- data stored on removable media will be locked away securely when not in use
- data is only stored on designated encrypted drivers and servers, and only uploaded to approved cloud computing services
- MOHS servers containing personal data are sited in a secure location, away from general office space
- data is backed up every 15 minutes with an offsite back up performed every night. These backups are tested monthly, in line with the company's standard backup procedures.
- all servers and computers containing data are protected by approved security software and a firewall.

Data use

Personal data is of no value to MOHS 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 will ensure their computer screens are always locked and password protected when left unattended.

Personal data will not be shared informally. In particular, it will never be sent by email as this form of communication is not secure.

Data is encrypted before being transferred electronically.

Personal data is never transferred outside the European Economic area.

Employees will not save copies of personal data to their own computers.

Data accuracy

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

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

Data will be held in as few places as necessary. Staff will not create any unnecessary additional data sets.

Employees will take every opportunity to ensure data is updated eg by confirming a customer's details when they call.

MOHS will make it easy for data subjects to update the information MOHS holds about them.

Data will be updated as inaccuracies are discovered eg, if a customer can no longer be reached on their stored telephone number, it will be removed from the database.

It is the Digital Marketing Executive's responsibility to ensure marketing databases are checked against industry suppression files every six months.

SAR (Subject access requests)

Individuals who are the subject of personal data held by MOHS are entitled to:

- ask what information MOHS holds on them and why
- ask how to gain access to it
- be informed as to how it is kept up to date
- be informed as to how MOHS is meeting its data protection obligations

If an individual contacts MOHS to request personal data, it is called a SAR (subject access request).

SARs from individuals should be made by email addressed to MOHS's data protection officer (helenhooper@mohs.co.uk).

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

Individuals will not be charged for this request. The data protection officer will provide the relevant data within 30 days. For instances where the data to be provided is excessive, the data protection officer will write to the individual to request additional time.

The data protection officer will always verify the identity of anyone making a SAR before handing over any information.

Providing information

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

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

To this end MOHS has a privacy statement, which sets out how data relating to this individual is used by the company.

Policy prepared by: Helen Hooper, CEO, MOHS Approved by the management team: 19th April 2018

Policy became operational on: 1st May 2018

Last reviewed: November 28th 2024