Data protection policy

Context and overview

Key details

- Policy prepared by: Michael Ray.
- Approved by committee of trustees on: 29/06/2017.
- Policy adopted on: 29/06/2017.
- Next review date: dd/mm/yyyy.

Introduction

weySight needs to gather and use certain information about individuals. These can include staff, members, suppliers, business contacts, 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 weySight's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures weySight:

- Complies with data protection law and follows good practice .
- Protects the rights of staff, members and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Terms

Herein the term 'staff' is taken to mean the class facilitator, trustees and volunteers past and present, and any other such person appointed by the committee of trustees in accordance with the constitution of weySight to perform administrative or other such roles as may be defined by the committee of trustees.

Data protection law

The Data Protection Act 1998 describes how organisations - including weySight - 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:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Be 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.

People, risks and responsibilities

Policy scope

This policy applies to:

- The registered office of weySight.
- All staff of weySight.
- All contractors, suppliers and other people working on behalf of weySight.

It applies to all data that weySight 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' activity within weySight.

Data protection risks

This policy helps to protect weySight 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, weySight could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with weySight has some responsibility for ensuring data is collected, stored and handled appropriately.

Each staff member 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 committee of trustees is ultimately responsible for ensuring that weySight meets its legal obligations.

The class facilitator is responsible for:

- Keeping the committee of trustees 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 weySight 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.
- 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.
- 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 and other initiatives abide by data protection principles.

Periodic review of this policy and related documents, particularly the subject access request documents, may be delegated by the class facilitator to a member of the committee of trustees, on agreement by the committee at any formal meeting.

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, staff members can request it from the class facilitator.

weySight will provide training to all staff to help them understand their responsibilities when handling data.

Staff 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 organisation 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.

Staff should request help from the class facilitator or the committee of trustees 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 class facilitator or committee of trustees:

- Ordinary members of weySight should not be given access to the data, other than their own personal data in response to a subject access request.
- 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 for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Staff should make sure paper and prints are not left where unauthorised people could see them, such as in the output hopper of a printer, or left on a table or other surface in the class venue.
- Data prints 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 between members of staff.
- 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 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.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones other than those used by the class facilitator.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to weySight unless it 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, members of staff 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.

- Data must be encrypted before being transferred electronically. The class facilitator can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Members of staff should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires weySight 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 weySight should put into ensuring its accuracy.

It is the responsibility of all staff 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 an ordinary member's details when they call.

weySight will make it easy for data subjects to instruct weySight to update their data in accordance with their wishes.

weySight will not cause data other than anything agreed with a subject to be displayed on a Web page, newsgroup, social media system or any other electronic system capable of being viewed by the general public.

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.

Subject access requests

All individuals who are the subject of personal data held by weySight are entitled to:

- Ask what information weySight holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how weySight is meeting its data protection obligations.

If an individual contacts weySight requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the class facilitator at the email address published by the committee of trustees for the same, or by telephone on the telephone number published by the committee of trustees for the same. The class facilitator can supply a standard request form, although individuals do not have to use this form.

Individuals will not be charged for a subject access request. The class facilitator will aim to

provide the relevant data within 14 days.

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

A response to a subject access request will be presented in a format which is accessible to the subject, for example in regular print, large print, Braille or verbally either in person or over the telephone.

The class facilitator may contact the subject before a response is compiled to ascertain the desired format of the response.

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, weySight will disclose requested data. However, the class facilitator will ensure the request is legitimate, seeking assistance from the committee of trustees and from legal advisers where necessary.

Providing information

weySight 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, weySight has a privacy statement, setting out how data relating to individuals is used by the company.

The privacy statement will be available on request. A version of the statement is also available on the company's website.