Portobello Eyecare Data Protection Policy – Data Protection Act 1998

Context & Overview

Key Details

- Policy Prepared By: Rudi Mccarthy
- Date Created: 9/11/2020
- Next Review: 8/11/2022

Introduction

Portobello Eyecare needs to gather and use certain information about individuals and companies.

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 comply with legislation.

Why this policy exists

This data protection policy ensure Portobello Eyecare:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers
- Is open how it store 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 Portobello Eyecare must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or in other ways.

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 that necessary
6. 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 & Responsibilities

Policy Scope

This policy applies to:

- Portobello Eyecare, 3 Portobello Parade, Fawkham Road, West Kingsdown, Sevenoaks, Kent TN15 6JP
- All staff and volunteers of Portobello Eyecare
- All contractors, suppliers and other people working on behalf of Portobello Eyecare.

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
- Plus other information relating to individuals

Data Protection Risks

This policy helps protect Portobello Eyecare from some 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 hacker successfully gained access to sensitive data.

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

Each person that handles personal data must ensure that it is handled ad processed in line with this policy and data protection principles.

However, this people have key areas of responsibility:

- The Data Protection Officer (DPO) **Rudi Mccarthy** is responsible for:
    - Keeping notice board 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 the policy.
    - Handling data protection questions from staff and anyone else covered by the policy.
    - Dealing with requests from individuals to see the data Portobello Eyecare holds about them.
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- **Rudi Mccarthy** 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

- **Rudi Mccarthy** 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 outlet such as newspapers.
    - Where necessary, working with other staff to ensure marketing

initiatives abide by data protection principles.

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 access it from their manager.
- Portobello Eyecare 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 guidelines.
- In particular, strong passwords must be used and the 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 to be found to be out of date. If no longer required, it should be deleted and disposed of in the correct manner.
- Employees should request help from their 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 Protection Officer.

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 be 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 a printer.
- 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 between employees.
- If data is stored on removable media (cd/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 an 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 regularly tested, in line with the company's standard back up procedure.
- Data should never be saved directly to laptops or other mobile devices such as tablets or smart phones.
- 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 Portobello Eyecare 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 screens are 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 manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside the EEA
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of the data.

Data Accuracy

The law requires Rudi Mccarthy 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 Portobello Eyecare 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 an unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance by confirming a customers details when they call.
- Portobello Eyecare will make it easy for data subjects to update the information Portobello Eyecare holds about them. For instance, via our 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 their database.
- It is the managers responsibility to ensure marketing databases are checked against industry suppression files every 6 months.

Subject Access Requests

All individuals who are subject of personal data held by Portobello Eyecare 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 Protection Officer at info@portobelloeyecare.co.uk The data protection officer can supply a standard request form, although individuals do not have to use this.

The information will be provided free of charge within 30 days. Where requests are manifestly unfounded or excessive a reasonable fee will be charged, taking into account the administrative costs of providing the information.

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

Disclosing Data For Other Reasons
In certain circumstance, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Portobello Eyecare will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance or advice where necessary.

Providing Information
Portobello Eyecare 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

How Long Will Patient Records Be Securely Held
Portobello Eyecare will hold all patient records both paper and electronic data for 10 years. This is with the exception of children under 16 where their records will be retained until their 25th birthday.

The legal basis for processing patient records is : legitimate interest and for the purposes of health care.

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