Davies & Jones Optometrists

Taking care of your personal information

The information we collect about you

We'll only ever collect the information we need to provide you with our services and manage our business.
We'll collect information from you or if you contact us on behalf of someone else, we'll collect information about the other person from you.
E.g. If you want to make an appointment, we will ask you for your name and contact details

How long we'll keep your information

We usually keep your information for the whole time you are one of our patients. We are legally obliged to securely store information for 10 years after your last appointment (or 10 years after a child's 18th birthday).

How we will use your information

We tend to use your information to tell you when your next appointment is due, keep you updated or if your spectacles or contact lenses are ready for collection.

You can choose to opt out of receiving communications at any time, simply by contacting us. We would also like to use your information to contact you about products and services offered by us and our service partners. If you choose to receive this, we'll only contact you in line with your preferences. You can change your preferences at any time.

L COMPANY LTD

Nature of work - Optician

Contact
Owain Mealing Tel 01443-682284 email owain@daviesandjonesoptometrists.co.uk
Davies & Jones Optometrists, 19 Hannah Street, Porth, RCT, CF39 9RB

Description of processing
The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information
We process personal information to enable us to provide healthcare services to our patients; promote and advertise our services; maintain our own accounts and records and to support and manage our employees Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.

Who the information is processed about
We process personal information about:

- patients
- customers
- suppliers and service providers
- consultants and other professional experts
- employees

Type/classes of information processed
We process information relevant to the above reasons/purposes. This information may include paper and/or electronic copies of:

- personal details
- referral letters, retinal images, visual field plots etc.
- family details
- lifestyle and social circumstances
- goods and services
- financial details
- education and employment details

We also process sensitive classes of information that may include physical or mental health details, racial or ethnic origin and religious or other beliefs.

Legal Basis for retaining patient information
Legitimate interest and for the purposes of health care

Legal basis for retaining customer information
Legitimate interest

Legal Basis for retaining staff information
Performance of a contract with the data subject or to take steps to enter into a contract and processing is necessary for carrying out obligations as an employer

Patient Data shared with
Registered health care professionals and those under their supervision

Customer information shared with
The data subject's bank

Staff personal data shared with
HR (including payroll) and senior management only

Time limits for erasure of patient information
The NHS specifies 7 years or, in the case of children under 18, until their 25th birthday for patients. College of Optometrists guidance is that it is best practice for records to be kept for 10 years. Only registered health care staff have access to the complete patient record. All registered staff comply with GOC standards, which ensure they respect patient confidentiality. Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role, all employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.

Time limits for erasure of customer information
Kept for tax purposes and future claims/information

Time limits for erasure of staff information
Kept for tax purposes and future claims/information

Technical/organisational measures to ensure patient data level of security appropriate to risk
Only registered health care staff have access to the complete patient record. All registered staff comply with GOC standards, which ensure they respect patient confidentiality. Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role, all employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date

Technical/organisational measures to ensure customer data level of security appropriate to risk
Paper records are kept securely. Electronic data is password protected; employees can only access the information essential for their role and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made; there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.

Technical/organisational measures to ensure staff data level of security appropriate to risk
Paper records are kept securely. Electronic data is password protected; employees can only access the information essential for their role and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made; there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.
Electronic records are backed up daily. Paper records are kept away from public access. Passwords are changes regularly. Anti-virus protection is kept up to date. All staff receive training on data protection.

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). 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.

Where necessary or required we share information with:

- healthcare professionals
- social and welfare organisations
- central government
- family, associates and representatives of the person whose personal data we are processing
- suppliers and service providers
- financial organisations
- current, past or prospective employers
- educators and examining bodies

Transfers
It may sometimes be necessary to transfer personal information overseas. When this is needed information is only shared within the European Economic Area (EEA). Any transfers made will be in full compliance with all aspects of the data protection act and GDPR

Statement of exempt processing:
This data controller also processes personal data which is exempt from notification