Privacy

Smiles Better privacy notice

Who we are

Smiles Better is committed to ensuring that we are transparent about the ways in which we use your personal information and that we have the right controls in place to ensure it is used responsibly and is kept safe from inappropriate access, theft or misuse.

We provide denture services as well as administrative activities. These include designing, manufacturing and fitting dentures.

This notice explains how Smiles Better will use your personal information and tells you about your privacy rights and how the law protects you. To find out how Smiles Better uses your personal information please access the bottom of our webpage.

What is personal information?

Personal information can be anything that identifies and relates to a living person. This can include information that when linked with other information, allows a person to be uniquely identified. For example, this could be your name and contact details.

The law treats some types of personal information as 'special' because the information requires more protection due to its sensitivity. This information consists of:

- Full name including title
- Date of Birth
- Address
- Contact Information
- Treatment
- Medical History
- Payment Information
- Clinical Notes
- Gender
- Appointment Information

Purposes

Your personal information may be collected and used for the following:

Generally, we may need to use some information about you:

- To refer patients to dental practices
- When dealing with finance companies
- Dealing with complaints
- To work with the GDC or DCS

- Court order
- For patient recalls or appointment scheduling
- to improve the general experience of our customers and of visitors to our websites
- for managing any online transactions you may elect to make and/or marketing choices or preferences you may have expressed (with consent)
- for archiving, research, or statistical purposes (including research and evaluation undertaken by the Smiles Better)

Legal basis for processing

Generally we collect personal information where:

- you, or your legal representative, have given consent
- you have entered into a contract with us
- it is required by law (such as where this is mandated by statute or under a court order)
- it is necessary to perform statutory functions (including law enforcement functions)
- it is necessary to deliver health services
- it is necessary to protect you or others from harm (e.g.in an emergency or civil disaster)
- it is necessary to protect public health
- it is necessary for exercising or defending legal rights
- you have made your information publicly available
- it is necessary for archiving, research, or statistical purposes
- it is necessary in the substantial public interest for wider societal benefits and is authorised by law
- it is necessary for fraud prevention and the protection of public funds
- when it is in our legitimate interests (or those of a third party) provided your interests and fundamental rights do not override those interests.

Your personal information may also be shared with other organisations, such as those who assist us in providing services and those who perform technical operations such as data storage and hosting on our behalf.

These practical arrangements and the laws governing the sharing and disclosure of personal information often differ from one service to another.

For this reason, each of our key service areas provides additional information about how we collect and use your information. These notices explain:

- why we need your information
- who else we obtain or receive it from
- the legal basis for collection and the choices you have
- who we share it with and why
- whether decisions which legally affect you are made solely using machine based technologies
- how long we keep your information
- how to exercise your rights

Data Transfers beyond EEA

We will only send your data outside the European Economic Area ('EEA'):

- with your consent, or
- to comply with a lawful and legitimate request, or
- if we use service providers or contractors in non EEA countries.

If we do transfer your information beyond the EEA, we will make sure that it is protected in the same way as if it was being used in the EEA. We will use one of these safeguards:

- Transfer it to a non EEA country with privacy laws that give the same protection as the EEA. Learn more on European Commission - Data protection.
- Put in place a contract with the recipient that means they must protect it to the same standards as the EEA. More information is available on European Commission - Data protection.
- Transfer it to organisations that are part of the Privacy Shield. This is a framework that sets privacy standards for data sent between the US and EU countries. It makes sure those standards are similar to what is used within the EEA. You can find out more about the Privacy Shield on European Commission - EU-US privacy shield.

If we propose to make a transfer in response to a lawful and legitimate request we will normally tell you in advance unless there are compelling reasons, such as law enforcement or, reasons of safety which justify not doing so.

Automated decisions

If we make a decision which legally affects you by using a computerised system or programme that does not involve a human being, our service specific privacy notices will explain this.

Data retention / criteria

We will only keep your personal information for as long as the law specifies or where the law does not specify this, for the length of time we would need to hold onto your personal information having regard to the purpose for which it was obtained, the nature of the information, industry practice and the all surrounding circumstances including historical.

How we keep your information safe

We are committed to ensuring your personal information is safe and protected from accidental loss or alteration, inappropriate access, misuse or theft.

As well as technical, physical and organisational controls, we recognise that a well-trained, informed and security alert workforce minimises privacy risks from human error and/or threats from malicious actors.

We require our service providers to implement appropriate industry standard security measures and only permit them to process your personal information for specified purposes in accordance with our contractual instructions.

Rights of individuals

You may exercise the rights listed below in relation to the council's use of your personal information.

Some rights are absolute and others are not.

To find out more about how these rights apply in particular circumstances, please visit Information Commissioner's Office - Guide to the General Data Protection Regulation.

To exercise these rights, please contact us (see below).

- **Access**
  You may request a copy of the personal information we hold about you.
- **Rectification and erasure**
  You may request that we rectify or delete any of your personal information if you consider it is incomplete, factually incorrect, processed unlawfully or, is unnecessary or no longer needed.
- **Review of automated decision making**
  Where we use only an automated system or programme that does not involve a human being, you have the right to request that a decision which legally affects you is reviewed by an appropriate officer.
- **Objection**
  You may object, at any time, to your personal information being processed. This applies to processing:
  - carried out in performance of our statutory functions or in the public interest, including 'profiling' , whether or not profiling is partly or fully automated;
  - for direct marketing purposes
- **Restriction of processing**
  You may request restriction of processing (quarantining) of your personal information for certain reasons, such as, for example:
  - if you have objected to the processing or asked us for erasure and we need time to consider your request and let you know our decision
  - you require us to retain your information for the establishment, exercise or defence of your own legal rights
- **Data portability**
  In defined circumstances either where the processing relies on your consent or arises out of a legal contract, you may request we supply a copy of personal information that you have provided to us in a portable and machine readable format.
- **Right to withdraw consent**
  Where the legal reason for processing your personal information is based on your consent, you have the right to withdraw your consent at any time, without affecting the lawfulness of our processing prior to the withdrawal of your consent.
  If you wish to exercise your rights (as outlined above) or to raise a concern about the handling of your personal information by the council, please contact us (see below)
  Whether you are exercising your rights or raising a concern, you will normally need to include documents that prove your identity as well as a clear and precise description of your request or concern.
  We will process requests in accordance within the legislative framework and the statutory time scales and inform you should an extension of time be necessary.

Complaints (ICO)

If you are not satisfied with the way we have answered a request from you or handled your personal information, you have the right to make a complaint to the Information Commissioner who may be contacted at: Information Commissioner's Office - Make a complaint.

Related pages

- Service specific privacy notices
- Data protection and freedom of information
- Data protection legislation
- Subject Access Request - How to request personal information an organisation holds about you

Elsewhere on the web

- Information Commissioner's Office - Guide to the General Data Protection Regulation
- European Commission - Data protection
- European Commission - EU-US privacy shield