Elite Dental Practice
246 - 248 Ravenhill Road,
Belfast,
BT6 8GJ
028 9045 9696
www.elitedentalpractice.co.uk

General Data Protection Regulation (GDPR)
Data Protection Policy & Procedures for
Elite Dental Practice

Elite Dental Practice aims to comply with the General Data Protection Regulation (GDPR) which came into effect on 25th May 2018. This policy and the related procedures lay out how Elite Dental Practice complies with the GDPR. All team members must ensure they read, understand and comply with our policy and procedures in relation to GDPR.

Ensuring that individuals' personal information is processed in line with the requirements of the GDPR and that individuals' privacy is respected is imperative and all team members must give this a very high priority.
To comply with the GDPR and the UK Data Protection Act (2018), our practice has notified the Information Commissioner that personal information relating to patients and team members is processed and stored within our practice.

Data Protection Definitions

GDPR defines several roles and responsibilities and introduces some new roles and terminology. Team members must ensure they are familiar with these.
The following are relevant and are explained below:

Data Processing
Includes collecting the information about an individual, using it, storing it, securing it, disclosing it and destroying it etc. GDPR applies to all businesses and organisations and to all personal data held about individuals. In a dental practice this means patients, employed and self-employed team members, referrers, and anyone else that the practice processes data for.

Data Controller
A data controller determines the purposes and means of processing personal data. This is the practice owner. In our practice this is the Practice owner

Data Processor
A data processor is responsible for processing personal data on behalf of a controller. Data processors are required to maintain records of personal data and processing activities and they have legal liability if they are responsible for a breach. All practice team members are data processors. The employer Dr Lida Fartash is responsible for making all team members aware of their responsibilities in relation to data protection. The need to comply with GDPR and other data protection laws is included in all employment contracts and associate agreements.
Data processors are also the practice management software companies, IT support companies, payment plan providers and all other organisations that handle personal data on behalf of the controller.

Data Subject
An individual for whom we process personal information.

Personal Data
Name, address, date of birth, doctor's name and address etc. The personal and the sensitive (including special category) data we process for our patients and team members is listed in our data inventories, GDPR Inventory Patients and GDPR Inventory Staff which are located in the main office.

Special Category Data
Includes sensitive information such as medical history, medical and dental records, ethnic origin, race, political opinions, religion, trade union membership, genetics, biometrics, health, sex and sexual orientation. It also includes DBS checks, Hepatitis B status.

Unauthorised Access
If someone who is not entitled to see details of another individual's personal data can obtain access without permission, this is unauthorised access and a breach of GDPR.

Personal Privacy Rights
Under GDPR, all individuals who have personal data held about them have the following personal privacy rights:
- Right to subject access
- Right to have inaccuracies deleted
- Right to have information erased
- Right to object to direct marketing
- Right to restrict the processing of their information, including automated decision making
- Right to data portability

Automated Decision Making
This includes all decisions made without human intervention e.g. email reminders to book an appointment or text or email reminders of appointments, direct marketing i.e. all decisions that are taken automatically.

Data Portability
The ability to take personal data elsewhere e.g. to another dental practice or employer.
Legal Basis for Processing Data
There are six legal bases for processing personal data and we are required to be able to justify and articulate the legal basis on which we collect and process all personal data that we hold. We must also document the legal basis on which we collect and process all personal data that we hold.

Data Protection Impact Assessment
A data protection impact assessment is the process of systematically considering the impact on privacy any project or initiative could have on the privacy of individuals.

Data Protection by Design and Default
The GDPR requires everything we do to be 'designed' with privacy in mind and it requires this to be our 'default' position.
Data protection by design and default means that everything we do or plan to do such as new projects and initiatives is always planned and executed with privacy in mind.

Data Protection Officer (DPO)
A DPO is a person designated or appointed to ensure the organisation or business complies with GDPR.
In our practice the DPO is the Practice Owner

GDPR Principles

Elite Dental Practice aims to comply with GDPR requirements which state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and kept up to date (inaccurate personal data must be erased or rectified without delay)
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

GDPR Practice Procedures

Risk Management

We have reviewed and enhanced our data protection risk management processes and recorded our actions on our GDPR risk assessment template. We undertake annual data protection risk assessments and follow up to ensure actions have been completed. GDPR compliance is discussed at our practice meetings as and when new information relating to the GDPR arises and actions arising are recorded and followed up. Practice meeting is carried out last Tuesday of each month.

Risk management protocols

All team members must ensure that they:

- Do not leave people's information in public view on the reception desk
- Lock filing cabinets when the practice is unattended
- Do not leave data displayed on computer/laptop screen (use a screensaver)
- Ensure that PC/laptop screen cannot be seen by anyone who is not entitled to see it
- Do not leave their computer logged on and unattended
- Change the password frequently
- Do not choose a password that's easy to guess
- Do not give the password to anyone, ever
- Do not disclose any personal information without the data subject’s consent or verifying the enquirer (e.g. phone the police officer or the social worker back via the station or office switch board)
- Are aware that email can be a very risky means of communicating, especially in relation to personal information
- Are careful when responding to email e.g. using ‘reply all’ or ‘send to all’ or when forwarding email
- Do not send sensitive personal information by email unless it is encrypted or anonymised
- Do not mix personal and work email accounts
- Understand that the need to maintain confidentiality forms part of their employment contracts and/or self-employed associate agreements
- Ensure that all paper waste containing any personal or confidential information is shredded securely.

Personal data inventories of patients and team members

Our personal data inventories list all the personal data we process for patients and team members together with the risks attached to each type of data.
As required by GDPR, the data inventories also list:

- Why we are you holding the data
- How we obtained it
- The retention periods
- How secure it is in terms of encryption and accessibility
- Whether it is ever shared with third parties and if so, on what basis
- Our legal basis for processing the personal data
- Whether we ever transfer the data outside the practice e.g. laboratory work
- How aware we have made the patient or team member that we are processing each piece of data.

Privacy Policy and Privacy Notices

As required by the GDPR we have a Privacy Policy for patient data that lays out what data we collect and process and we have Privacy Notices that alert staff and patients to the collection of their data.
Our Privacy Policy and our Privacy Notices contain the following essential information:

- Our identity
- Our reasons for gathering the data
- The use it will be put to
- Who it will be disclosed to
- Our legal basis for processing the information
- The retention periods
- The right to complain
- Whether their data will be subject to automated decision-making
- Individuals' rights under the GDPR.

This information is provided in concise, easy to understand and clear language.

Access Rights

Access to records

All data subjects have the right of access to and copies of their personal data whether they are held on paper or on computer.

Patient records

A request from a patient to see records or for a copy must be referred to the patient's dentist.
Care should be taken to ensure that the individual seeking access is the patient in question and where necessary the practice will seek information from the patient to confirm identity. A copy of the record must be supplied within one month at the very latest from the request being made. Every effort should be made to supply the information requested without delay and as soon as possible following receipt of the request.
The fact that patients have the right of access to their records makes it essential that information is properly recorded.
Records must be:

- Contemporaneous and dated.
- Accurate and comprehensive.
- Signed by the dentist.
- Strictly necessary for the purpose.
- Not derogatory.
- Such that disclosure to the patient would be unproblematic.

We have processes in place to ensure that we can respond to a data subject's request for access to or copies of their records within one month (four weeks). We do not charge a fee for access to or copies of records. In some situations, we may refuse an access request if we think it is unfounded or excessive. In those situations, we have clear

refusal policies and procedures in place and will always ensure we can demonstrate why the request meets these criteria.
We provide additional information to people making requests, including our data retention periods and the right to have inaccurate data corrected.

Access refusal policy

Under certain, very limited circumstances we may refuse access to or copies of personal records.
These could include:

- Where we have concerns about safety or a safeguarding concern.
- Excessive or repeated requests for the same information that has already been provided.

In these circumstances we will demonstrate how the request fits these criteria in accordance with GDPR and we will provide the individual with an explanation for the refusal unless this could put them at risk.

The six legal bases

We understand there are six legal bases for processing personal data. We have considered the legal basis on which we process all the personal data we hold and have documented this in our Privacy Policy and our Privacy Notices. We will include the legal basis in our data protection impact assessments. The legal basis is also recorded on our data inventory templates.

Consent to data processing

Consent is one of the legal bases for processing personal data. Consent is not appropriate as a legal basis for processing personal data in relation to patient care or to administer an employment contract or a self-employed associate agreement.
Consent must always be obtained for direct marketing.
We also obtain consent for the following:

- Telephone number for appointment reminders
- Emails for appointment reminders to ask a patient to book an appointment
- Taking and using photographs
- Sharing personal information with a referral practice
- Sharing information relating to appointment details, treatment details or costs with a named individual.

Gaining Consent

We understand that gaining consent is a complex process and we ensure that all the conditions described below are satisfied.
When using consent to process data for the purposes listed above, we ensure that:

- Consent is freely given, specific, informed and unambiguous
- Patients and team members are never forced into consent, nor are they unaware that we are processing their personal data
- They know exactly what they are consenting to and we take precautions to ensure there can be no doubt that they are consenting
- Consent is always obtained by a positive indication of agreement, it is never inferred from silence, pre-ticked boxes or inactivity
- Consent is verifiable, and individuals are informed in advance of their right to withdraw consent
- We can demonstrate that consent was given, and we have an effective audit trail.

Reporting Data Breaches

All breaches must be reported to the Data Protection Commissioner (DPC) within 72 hours unless the data was anonymised or encrypted. Breaches that might bring harm to an individual (e.g. identity theft or breach of confidentiality) must also be reported to the individual(s) concerned.
We have procedures in place to detect, report and investigate a personal data breach.
All team members understand that they must inform Practice owner or Practice Manager.
If, after investigation, a team member is found to have breached data protection and not reported it, he or she shall be liable to summary dismissal in accordance with our practice disciplinary policy.

Data Protection Impact Assessments and data protection by default and design

A Data Protection Impact Assessment (DPIA) is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals.
We always adopt the approach of privacy by design as our default approach. Prior to embarking on any project or initiative we always undertake a data impact assessment to identify potential privacy issues before they arise to enable us to find ways to mitigate any issues. If we cannot reduce the impact sufficiently, we would not proceed.
Our systematic considerations together with the measures to be put in place to mitigate any risks to privacy are recorded in GDPR Folder in main office.

Data Protection Officer (DPO)

Our DPO is Dr Lida Fartash
Our DPO's duties are:

- To inform and advise the practice and its employees about our obligations to comply with GDPR and other data protection laws
- To monitor compliance with GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- To be the first point of contact for individuals whose data is processed, e.g. patients, employees, associates and supervisory authorities.

Note: A DPO should probably not be the practice owner (the data controller) because of the potential for conflicts of interest. A DPO can be an employee, provided that person is given appropriate training and autonomy to be able to undertake the duties described above. The role can also be outsourced.

Security of Information

Personal data about our patients and team members is held in the practice's computer system and/or in a manual filing system. The information is only accessible to authorised team members. Our computer system has secure audit trails and we back up information routinely. Paper records are stored in lockable, fire-proof cabinets that are locked when the practice is unattended.

Personal Information - patients

Personal information about our patients includes:

- The patient's name, current and previous addresses, bank account/credit card details, telephone number/e-mail address and other means of personal identification such as his or her physical description.
- Information that the individual is or has been a patient of the practice or attended, cancelled or failed to attend an appointment on a certain day.
- Information concerning the patient's medical history, including their physical and/or mental condition and their oral health or condition.
- Information about discussions undertaken and agreements reached on treatment options, including costs of any proposed treatment.
- Information about the treatment that is planned, is being undertaken or has been provided.

- Information about family members and personal circumstances supplied by the patient or others.
- The amount that was paid for treatment, the amount owing, or the fact that the patient is a debtor to the practice.

Personal Information – team members
The personal information we hold on our team members is listed in our Data Inventory which is stored in the main office and to which all team members have access.

Retention Periods

Elite Dental Practice retains records of personal data only for as long as is required for the purposes for which it was collected or as required by law or to comply with statutory requirements.
Retention periods for individual items of data are documented in our Data Inventory records, in our Privacy Policy and in our Privacy Notices as required by the GDPR.

Retention – team members

We will retain team members' personal information only for as long as we need to in order to fulfil the purposes for which it was collected. After our working relationship has terminated we will retain team members' personal data for [Insert your retention period having taken formal HR advice].

Retention – patients

This practice retains dental records and orthodontic study models while the patient is a patient of the practice and after they cease to be a patient, for at least eleven years, or for children until age 25, whichever is the longer.

Sending of Information Electronically

To comply with GDC Standards and GDPR, we ensure that if we are sending confidential information, we use a secure method. If we are sending or storing confidential information electronically, we will ensure that it is encrypted.
Disclosure of Information to Third Parties
The information we collect, and store will not be disclosed to anyone who does not need to see it.

Disclosure of Information – team members

We will share our team members' personal information with third parties when required by law or where it is necessary to administer the working relationship with them or where we have another legitimate interest for doing so.
Third parties we may share team members' personal information with may include:

- Payroll providers
- Our accountants
- Human resource management providers
- Patient payment plan providers
- Regulatory authorities such as the General Dental Council or the Regulation and Quality Improvement Authority of Northern Ireland (RQIA)
- NHS Local Authorities
- Dental payment plan administrators
- Insurance companies
- Fraud prevention agencies
- In the event of a possible sale of the practice at some time in the future.

We may also share personal information where we consider it to be in a team member's best interests or if we have reason to believe an individual may be at risk of harm or abuse.

Disclosure of Information - patients

The information we collect, and store will not be disclosed to anyone who does not need to see it.

We will share our patients' personal information with third parties when required by law or to enable us to deliver a service to them or where we have another legitimate reason for doing so. Third parties we may share patients' personal information with may include:

- Regulatory authorities such as the General Dental Council or or the Regulation and Quality Improvement Authority of Northern Ireland (RQIA)
- NHS Local Authorities
- Dental payment plan administrators
- Insurance companies
- Loss assessors
- Fraud prevention agencies
- In the event of a possible sale of the practice at some time in the future.

We may also share personal information where we consider it to be in a patient's best interest or if we have reason to believe an individual may be at risk of harm or abuse.

Right to Object

Data subjects have the right to object to their personal data being processed or disclosed. Patients and team members who wish to object should discuss the matter with the Practice Owner/Manager. This may affect our ability to provide patients with dental care or it may affect our ability to fulfil the contract or agreement we hold with a team member.

Code of Practice for Confidentiality and Data Protection

Elite Dental Practice requires all team members to comply with the principles of GDPR and this Code of Practice.

Practice team members must:

- Never name a patient or team member or discuss identifiable information about a patient or team member outside the practice, including with friends or relatives of the patient or team member.
- Store patient records securely and confidentially where it is not possible for other patients or individuals to read them.
- Lock computers when not in use.
- Store paper records in lockable filing cabinets that are locked when the practice is unattended.
- Not give a school information about whether a child attended for an appointment on a particular day. It should be suggested that the child is asked to obtain the dentist's signature on his or her appointment card to signify attendance.
- Not provide information about a patient's appointment record to a patient's employer.
- Ensure that when talking to a patient on the telephone or in person in a public area, other patients cannot overhear sensitive information.
- Ensure that discussions about patients do not take place in the practice's public areas.
- Ensure that messages about a patient's care are not left with third parties or left on answering machines. A message to call the practice is all that can be left.
- Ensure that password-protected computer records are backed-up every day, with back-ups stored away from the practice.
- Change your password frequently and do not choose a password that is easy to guess.
- Keep your password secret and do not give it to anyone else at any time.
- Ensure the appointment book and day list are not visible to patients or anyone not involved in patient care.
- Never disclose patient information to a third party without consent, including confirming that someone is a patient at the practice or that they have an appointment. This includes disclosure of appointment books, day sheets or

computer screens to police officers or Inland Revenue officials, unless on the specific instructions of the dentist.

- Post all written communications, including recalls or reminders, in an envelope
- If called upon to demonstrate the practice's administrative/computer systems do not allow actual patient information to be used.
- Ensure that if you are sending confidential information, you use a secure method.

If you are sending or storing confidential information electronically, you should ensure that it is encrypted.

This Policy, Code of Practice and the related practice procedures were implemented on: [24/05/2018]
This Policy, the Code of Practice and all related procedures will be reviewed annually and are due for review on: [24/05/2026] or prior to this date in accordance with new guidance or legislative changes.
All team members are required to read this policy and related procedures and sign to confirm they understand it and will comply with it at all times.

Signed:

Date: 13/2/25 Review: 13/2/28

Elite Dental Practice
246 - 248 Ravenhill Road,
Belfast,
BT6 8GJ
028 9045 9696
www.elitedentalpractice.co.uk