General Dental Council | protecting patients, regulating the dental team

DATA PROTECTION POLICY

Ref GDC-IT-POLICY-05

Definitions

Policy Application

This policy applies to all employees, temporary staff (such as agency and interim workers), Council Members, GDC Associates, contractors, and other authorised users of GDC information technology (IT) including all personnel affiliated with third parties, and to all equipment owned or leased by the GDC. “Associates” includes, but is not limited to, any non-Council members who are serving on Council committees or Task and Finish Groups, members of the Appointments Committee and Statutory Committees, Quality Assurance Inspectors, Specialist List Appeal Panellists, Registration Assessment Panellists, ORE Advisory Group members and panellists, and Dental Complaints Service Advisory Board members and panellists. Where the policy refers to “Council members” and / or “associates”, this means all those referred to in this paragraph unless it is otherwise indicated.

Purpose and Scope

This policy sets out the GDC approach to the obligations imposed on the GDC by the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (the DPA). It serves as the GDC’s ‘appropriate policy’ for the purposes of Schedule 1, Part 2, Paragraph 5 of the DPA.

This policy applies to personal data as defined by Article 4 of the GDPR; that is, any information relating to an identified or identifiable natural person. The GDPR extends the definition of personal data to include identification numbers, such as the GDC registration number, IP address and social media name.

It also covers information which on its own does not identify someone but which would identify them if put together with other information.

This policy also applies to special categories of personal data as defined by Article 9(1) of the GDPR (which includes information about physical and mental health and racial or ethnic origin) and data relating to criminal offences as defined in Article 10 of the GDPR. Special category personal data and criminal convictions etc data, is data that is particularly sensitive and therefore merits specific protection.

Financial information is not expressly defined as sensitive (or special category) personal data under the GDPR and the DPA but the GDC has a particular duty of care with regard to such information and considers that it should be classified as such and subject to the same safeguards.

Policy

Processing of personal data and special category personal data

The GDC is required to collect, process and retain personal data (including special category personal data) to comply with its legal, regulatory and operational obligations. It includes information about:

- current, past and prospective registrants;
- current, past and prospective users (including contractors or temporary users) of GDC IT systems, software and information stored in or accessed through them or through systems operated by third parties;
- current, past and prospective Council members and associates;
- current and previous informants, witnesses and experts involved in the Fitness to Practise process;
- enquirers who contact the GDC;
- personnel in, and personal data received from, external organisations with whom the GDC has relationships, for example Government departments, NHS bodies, other statutory and regulatory bodies, such as the PSA, and suppliers;
- Employees, including contractors;
- Job applicants;
- External experts, consultants and advisers;
- Respondents and their responses to consultations and surveys;
- Journalists and the media.

This personal data, whether held on paper or electronically is subject to the safeguards set out in the GDPR and the DPA.

Examples of personal data processed by the GDC

- Names of individuals
- Registration numbers
- Contact information (for example postal address, registered address, telephone number, email address)
- Date of birth, passport number, nationality
- Occupation or job title
- Places of work
- Information about an individual's education and qualifications

- Information about an individual's skills and expertise

Examples of special category personal data processed by the GDC

- Physical or health details
- Racial or ethnic origin
- Religious or other beliefs
- Political opinions
- Sexual life
- Trade union membership
- Genetic or biometric data

Criminal offence data

The GDC may process personal data relating to the commission or alleged commission of a criminal offence by an individual and legal proceedings, outcomes and sentences convictions in respect of such offences to the extent that such matters are relevant to the GDC's functions regarding the dental professionals it regulates.

The GDC may also be provided with this information by a prospective employee as part of their application and or as part of the pre-appointment process.

Data Subject Rights

An individual's rights under the GDPR are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to object
- The right to restrict processing
- The right to data portability
- Rights in relation to automated decision making and profiling.

The GDC's Data Subjects Rights Policy outlines what the GDC does to ensure the rights of the individual under the GDPR are respected and responded to appropriately.

More information about how the GDC manages and responds to subject access requests can also be found here: https://www.gdc-uk.org/about/freedom-of-information.

Principles relating to processing of personal data

The current principles as set out in Article 5 of the General Data Protection Regulation and part 3, chapter 2 of the Data Protection Act 2018 apply to this policy.

1. Personal data must be:

    a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

    f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

GDC Compliance

The GDC, as data controller, is responsible for, and must be able to demonstrate compliance with these principles. We follow procedures to ensure that all

employees, contractors, agents, consultants and other parties who have access to any personal data held by or on behalf of us are fully aware of, and abide by, their duties and responsibilities under data protection legislation.

In order to meet the requirements of the data protection principles, the GDC must:

- observe fully the conditions regarding the fair collection and use of personal & special category personal data
- when asking for information which includes personal data and special category data, make clear the purposes for which the GDC will use that information
- collect and process personal data and special category personal data only to the extent that it is needed to fulfil operational or any legal requirements
- ensure the quality and accuracy of personal data used
- ensure that information is held for no longer than is necessary
- ensure that the rights of individuals whose personal data is held can be fully exercised under the Act
- take the appropriate technical and organisational security measures to safeguard personal data and special category personal data
- ensure that personal data is not transferred outside the EEA without suitable safeguards.

All users of GDC information have responsibilities in relation to data security which are set out in more detail in the Information Governance Policy and supporting policies, Information Security policy and other IT policies.

Information (personal data and special category data) will be retained and reviewed for disposal in line with the GDC's retention schedule published on the GDC's website here.

All users of GDC information are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Some of the ways in which the GDC protects personal data include:

- Having a dedicated person with specific responsibility for data protection in the GDC
- Providing annual awareness training to employees in the handling of personal data
- Providing training in data protection and security to all new staff.
- Ensuring all users of GDC information only have access to the personal

data they need to in order to carry out their duties

- Carrying out reviews and audits which consider the way personal data is managed and accessed
- Ensuring appropriate technical and organisational measures are in place to protect the confidentiality, integrity and availability of information
- Undertaking regular and on-going reviews of security and cyber risks
- Carrying out annual IT Health Checks and penetration testing
- Using Data Protection Impact Assessments (DPIAs) to ensure privacy issues are considered from the outset
- Regularly reviewing the GDC information assurance and security policies and procedures.
- Maintaining records and logs of processing activity (e.g. information asset register, personal data register, security incident log, risk register)
- Publishing a retention schedule which states how long we will retain types of personal data
- Providing regular training and awareness for staff on information assurance and security
- Using the government Supplier Assurance Framework and Crown Commercial Services frameworks where possible when working with suppliers and third parties
- Ensure contracts which involve any storage or processing of personal data on behalf of the GDC contain provisions which comply with the mandatory Article 28 of GDPR data processor requirements.
- Seek GDC IT advice, and approval, before considering a supplier whose operations involve any storage or processing of personal data outside the EU.

Reporting data security incidents

The GDC is required to have adequate technical and organisational measures in place to protect personal data and has a reporting system in place which ensures that we not only identify personal data breaches but that we learn from them to improve our systems and processes.

A Data Security Incident (DSI) is a reported concern about the use, access, destruction of personal data. This does not only mean incidents where something has happened but should also include 'near misses' where something almost happened.

Where a personal data breach has occurred it will fall into one or more of the following categories:

- there has been/almost been an unauthorised or accidental disclosure of, or access to, personal data.
- there has been/almost been an accidental or unauthorised loss of access to, or destruction of, personal data.
- there has been/almost been an unauthorised or accidental alteration of personal data

Incidents should be reported to the GDC's Information Governance Team as soon as we become aware of them so that we can take action to limit their impact and consider whether we should report the matter to the Information Commissioner, which is a decision made by the GDC Information Governance Manager and the GDC Senior Information Risk Owner (SIRO). Under the GDPR, we have a 72-hour window within which to take that decision.

Members of staff should inform their line managers immediately. The line manager will complete the Data Security Incident Reporting Form and send it to the Information Governance Team (DSI@gdc-uk.org), copying in their line manager.

The Information Governance Team will then liaise with the line manager or GDC associate contact to investigate the incident and provide advice on how best to respond.

Data security is one measure of individual performance that can and should be considered by line managers during 1:1s and as probation/part mid and final year performance reviews. Guidance to managers is available on the intranet here.

Related policies

Information Governance Policy and supporting policies

Data Subject Rights Policy

Document Control

Policy Ref: GDC-IT- POLICY – 05 – Data Protection Policy		
Author: GDC Corporate Legal	Authorised by: GDC Corporate Legal	
Version: 4.8	Effective Date: July 2016	Next Review: July 2020