General Dental Council

Data Protection Policy

Owner	Information Governance Team
Author	Information Governance Manager
Reviewed by	Head of Information Governance & Data Protection Officer
Effective from	16 August 2021(Included in IT Security Policy prior to 2021 and then included as a stand alone document under the Information Governance Team thereafter)
Approved by and date	SIRO – 7 August 2025
Review frequency	2 years
Review Date	07/08/2027

Version History

Review Date	Changes	Who
09/08/21	Separated policy from IT policies. Updated broken link. Changes to some wording ('UK GDPR' from 'GDPR')	Nick Insley
01/2025	Updated with reference to new Appropriate Policy Document and table added with Data Protection Principles	Katharine Schopflin
04/2025	Revisions and amendments to wording, change to sensitive data reference, table for meeting principles	Jake Smith
7/8/2025	SIRO approval	Katie Spears

1. Purpose and Scope

1.1. This policy sets out our approach to the obligations imposed on us by the UK General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (the DPA). By outlining the procedures for complying with the Article 5 UK GDPR Data Protection Principles, it provides an adjunct to the GDC's Appropriate Policy Document for the purposes of Schedule 1, Part 2, Paragraph 5 of the DPA 2018.

1.2. This policy applies to all GDC staff, including temporary staff, Council Members, Independent Governance Associates, the wider GDC Associates group, contractors, and other authorised users of our information technology (IT). It includes all personnel affiliated with third parties, and to all equipment owned or leased by the GDC.

1.3. The data covered in this policy applies to personal data as defined by Article 4 of the UK GDPR, that is, any information relating to an identified or identifiable natural person. The UK 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.

1.4. Special categories of personal data as defined by Article 9(1) of the UK 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 UK GDPR is also covered in this policy. Special category personal data and criminal conviction data is data that is particularly sensitive and therefore needs specific protection. For further information as to how the GDC processes this type of data, please see the 'Appropriate Policy Document for Special Category Data'.

1.5. Some information relating to an individual is sensitive due to its nature but is not expressly defined as special category personal data under the UK GDPR and the DPA. For example, financial information. Where information which may be sensitive due its nature is processed, this policy requires that we consider that sensitivity when ensuring it is processed in accordance with the data protection legislation, with business areas seeking support and advice from the Information Governance team.

2. Policy

2.1. Processing of personal data and special category personal data

2.1.1. 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 our IT systems, software and information stored in or accessed through them or through systems operated by third parties;

- current, past and prospective Council members, Independent Governance Associates and the wider Associates group;
- 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.

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

2.2. Examples of personal data processed by the GDC

- Names of individuals
- Registration numbers
- Contact information (for example, registered address, telephone number, email address)
- Date of birth, passport number, nationality
- Occupation or job title
- Fitness to practise history
- Registration history
- Information about an individual's education and qualifications
- Information about an individual's skills and expertise

2.3. 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/orientation

- Trade union membership
- Genetic or biometric data

2.4. Criminal offence data

2.4.1. 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. We process it to the extent that such matters are relevant to our functions regarding the dental professionals we regulate.

2.4.2. We 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.

2.4.3. For further information as to how we will process this data, please see the 'Appropriate Policy Document for Special Category Data'.

2.5. Data Subject Rights

2.5.1. An individual's rights under the UK GDPR are:

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

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

2.5.3. More information about how we manage and respond to subject access requests can also be found here: https://www.gdc-uk.org/about/freedom-of-information.

2.6. Principles relating to processing of personal data

2.6.1. The principles as set out in Article 5 of the UK GDPR 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 it 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). Providing this is done with the 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 (the GDC) shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

2.7. GDC Compliance

2.7.1. 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 and processes.

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

2.7.3. 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.

2.7.4. Personal data will be retained and reviewed for disposal in line with the GDC's asset register and retention schedule published on the GDC's website.

2.7.5. 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.

2.7.6. The table below outlines how the GDC meets each of the Article GDPR Principles:

Lawfulness, fairness and transparency • The GDC has identified lawful bases for its processing, outlined in the Records of Processing Activity, and further Schedule 1 conditions for processing Special Category (SC) and Criminal Conviction (CC) data, outlined in its Appropriate Policy Document • The GDC makes appropriate privacy information available via the Privacy Notice on the corporate website • We are transparent when we collect personal data and ensure that data subjects understand how their data will be used at the time that we collect it
Purpose Limitation • The GDC has clearly identified its purpose for processing SC and CC data and this is outlined in our Privacy Notice • When we plan to use personal data for a new purpose, we record this in a DPIA screening form and, where there is a potential high risk to the rights and freedoms of individuals, in a full-scale DPIA
Data Minimisation • We are satisfied that we only collect SC/CC personal data that we actually need for our specified purposes • This is recorded in our DPIAs and report requests

• Data is reviewed in accordance with the Corporate Records Retention Schedule, which is updated annually
Accuracy • Local standard operating procedures and system and process design ensure that the data we collect is accurate and kept up to date • We keep records of Individual Rights Requests to correct data
Storage Limitation • We carefully consider how long we keep SC/CC data and this is recorded in our Corporate Records Retention Schedule and Record of Processing Activities • Data is reviewed annually with reference to the Retention Schedule
Integrity and confidentiality (Security) • We analyse the risks to our processing and ensure the appropriate level of security is in place to protect our data, as outlined in our Information Security Policy • Technical measure and controls are put in place to meet the needs of SC/CC data • Where external processors are used, such as external platforms, we assess the third party's security measures
Accountability • We maintain a Record of Processing Activities and update it annually • We have a suite of appropriate policies to ensure the Data Protection Principles and rights of Data subjects are maintained • We carry out Data Protection Impact Assessments for all new processing with the potential to result in high risks to individuals' rights, and document all other new processing • We assess the GDC's performance against externally-mandated standards and guidance for best practice in Data Protection • Responsibility for data protection is held at the highest level of the organisation and there is clear guidance for Information Asset Owners as to their duties

2.8. Specific measures by which the GDC protects personal data include:

- Having a dedicated person and team 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
- Auditing the physical workspace for adherence to the clear desk policy
- 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 and continually for projects and change
- Regularly reviewing the GDC 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 an asset register and retention schedule which states where our assets are and 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.
- Have in place a robust procedure for reporting and mitigating Data Security Incidents

3. Related Policies

- Appropriate Policy Document for Special Category Data
- Information Governance Policy
- Data Subject Rights Policy

- Record of Processing Activities
- Corporate Records Retention Schedule
- Information Security Policy
- Data Security Incident Reporting Policy
- DPIA Policy and Guidance
- Information Asset Owner Policy

4. Monitoring and Review

This policy is reviewed every two years.

Its approval forum is the Senior Information Risk Officer. Any minor amendments may be made by the Head of Information Governance & Data Protection Officer.