Data Protection Policy

Authors:	Julian Graves
Version:	3.0
Status:	Issued
Date:	22 May 2018
Reference:	Data Protection Policy v3.0
Location:	

1. INTRODUCTION

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) aim to strike a balance between the privacy rights of individuals and the ability of organisations to use personal information to conduct their business.

The General Medical Council (GMC) needs to collect and use personal data to carry out our statutory responsibilities under the Medical Act 1983. The largest category of people we hold information about is doctors; but we also hold information about others, including those who raise concerns about doctors; current, past and prospective employees and contractors; and members of the Council. All personal information must be collected, stored, used and disposed of properly, in accordance with the principles of the GDPR and the DPA and other relevant privacy law, including the Human Rights Act 1998.

1.1 Purpose

The purpose of this policy is to set out the principles of data protection best practice which we will follow in our work, and to provide a managed framework for fulfilling our business needs, accountability and legal responsibility.

The GMC has a legal obligation to comply with the terms of the GDPR and the DPA as a data controller. Furthermore, since our core business revolves around the handling of personal data, much of it special category personal data, it is vital that we follow best practice to retain the public confidence necessary to carry out our regulatory responsibilities. For a full list of definitions see Appendix A.

1.2 Scope

This policy applies to all GMC staff, council members and associates.

1.3 Responsibilities

Information Policy Team

The Information Policy Team will work closely with colleagues to ensure there is consistency in the handling of personal data and that data protection advice, guidance and training is provided to staff and contractors where appropriate.

The Information Policy Team will also be responsible for considering individual rights requests (other than subject access requests) introduced by the GDPR and for providing advice to other directorates in relation to these rights.

Information Access Team

The Information Access Team is responsible for responding to subject access requests and for providing advice to other directorates to assist them in responding to related queries.

Information Security Working Group (ISWG)

The ISWG supports the information security management framework in operation under ISO27001. The key responsibilities of the group include:

- Approving and supporting the Information Security Management System
- Developing, approving and implementing GMC information security policies and procedures
- Supporting the Head of Information Security and Records Management responsible for coordinating the implementation of information security
- Reviewing status reports covering information security implementation, updates on risks, actioning recommendations following security reviews, audits etc.
- Reviewing and monitoring incident reports together with the results of any investigation carried out
- Recommending changes to wider policies and procedures based on security incidents and changes in risks
- Gaining and maintaining awareness of the information security risks being faced by the GMC in order to continually improve our systems and processes
- Acting as champions for information security in their own business area

Data Protection Officer (DPO)

The GDPR introduces the concept of a Data Protection Officer (DPO). The DPO's functions are set out in Art. 39 of the GDPR. These require the DPO to be involved on a day-to-day basis in data protection compliance and facilitating compliance through the implementation of tools such as data protection impact assessments, oversight of processing activities and additional subject rights processes.

Directors and managers

Directors and managers are responsible for ensuring that practices and systems in their areas comply with data protection legislation. Where non-compliant practices are identified, action will be required to be taken to ensure compliance.

Managers should consider the data protection implications of new policies and procedures to ensure that they are compliant with data protection legislation before implementing them, and can do so by undertaking a Data Protection Impact Assessment.

Associates and Contractors

Many people contribute to the work of the GMC. Where appropriate, the GMC will provide guidance and/or training to associates and contractors to make them aware of how they can comply with data protection legislation while they work with or for us.

The responsibility of associates and contractors to comply with data protection legislation will be made known to them when they begin working for the GMC, and periodically thereafter.

All staff

All staff are accountable to the organisation for compliance with this policy and with related policies, standards and guidance. All staff have a basic responsibility to handle personal data in accordance with data protection legislation. All staff are required to complete the mandatory data protection and information security eLearning training within the requisite timeframe.

Inappropriate processing of personal data may lead to or result in disciplinary action being taken.

1.4 Related Procedures

This policy has been formulated within the context of the following documents:

- Article 30 GDPR policy document
- Schedule 1, Part 4 DPA policy document
- Records management policy
- Records retention and disposal policy
- Information Security Policy
- Reporting Data Protection Breaches and Security Incidents Policy

1.5 Reference Documentation

- General Data Protection Regulation - (EU) 2016/679
- Data Protection Act 2018

2. POLICY

2.1 Information Commissioner's Office (ICO) funding

Data controllers, as defined by data protection legislation, are required to pay the ICO the requisite fee in order to assist with the funding of their regulatory activities. The ICO will publish the following details in relation to each controller who has paid a fee:

- The name and address of the controller
- Our data protection registration number
- The level of fee we have paid
- The date we paid the fee and when it is due to expire
- The name and contact details of our DPO

2.2 Data Protection Principles

When we process information we will comply with the requirements of the GDPR, the DPA, the Human Rights Act 1998, and common law duty of confidentiality.

We will consider the six data protection principles when processing personal data. The principles are as follows:

Principle 1 - **'Lawfulness, fairness and transparency':** Personal data is fairly, lawfully and transparently processed

Principle 2 - **'Purpose limitation':** Personal data is processed for limited purposes

Principle 3 - **'Data minimisation':** Personal data is adequate, relevant and limited to what is necessary

Principle 4 – **'Accuracy':** Personal data is accurate and kept up to date. Inaccurate data should be erased or rectified without delay

.

Principle 5 – **'Storage limitation':** Personal data should be kept in a form which permits identification of data subjects for no longer than necessary for the purpose of the processing. Personal data may be stored for longer periods if it is processed solely for archiving in public interest, scientific or historical research or statistical purposes.

Principle 6 – **'Integrity and confidentiality':** Personal data should be processed to ensure appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

Further information about each of these principles can be found on the Information Commissioner's Office website here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

2.3 Data subject rights

A data subject has certain rights conferred under the GDPR including:

- Request access to his or her personal data
- The right to be informed
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

An individual may make a request under any of these rights and the GMC will be required to respond within the statutory deadline of one calendar month unless the request meets the criteria to allow an extension of up to a further two calendar months.

Requestors should be aware that certain requests may not be complied with where an applicable exemption applies. We will provide an explanation in these circumstances.

2.4 Security

As required by GDPR data protection principle 6 we will take proportionate technical, physical and organisational measures to ensure that our sensitive information (including personal and special category personal data) is held securely and protected from destruction, loss, unauthorised access and disclosure.

2.5 Transfer of personal data

We will only transfer or store personal data outside the EEA where we are required to as part of our regulatory responsibilities, we are confident it is in the substantial public interest and otherwise where it is adequately protected:

We have assessed and found any risk in transferring the personal data is mitigated; and/or we have otherwise made the third party contractually aware of their responsibilities using appropriate contractual language.

2.6 Incident reporting

We recognise that mistakes happen and have implemented an internal policy to ensure that staff know what to do in the event of an inappropriate disclosure of information and potential breach of data protection legislation.

Advice is available to staff, who must report breaches in order for incidents to be assessed consistently. This message is reinforced in the mandatory data protection and information security eLearning package.

Breaches will be notified to the data subject and the Information Commissioner's Office (ICO) where required in line with ICO guidance. This will be determined by the Data Protection Officer.

2.7 Data Protection Impact Assessments

When we're doing something new, Data Protection Impact Assessments (DPIAs) help us think about any privacy and confidentiality issues before we start. We should think about the impact new initiatives (e.g. new project; new or changed policy; or new information sharing activity) will have on the people whose information we plan to use.

DPIAs allow us to identify potential risks at the start of a project and to develop a plan to manage and mitigate them. As well as helping us to avoid issues altogether, this approach can also save time and effort later if things do go wrong. DPIAs help to ensure that we are compliant with data protection legislation and the Human Rights Act.

DPIAs are an essential component of all GMC project work. We will seek to conduct a DPIA for initiatives involving:

- sharing data with external organisations
- asking external organisations to share data with us
- using existing data for a new purpose.

In addition the GDPR introduces a mandatory DPIA requirement for projects which, for example, introduce new technology or involve high risk personal data processing. The ICO's guidance sets out all the types of processing where the mandatory requirement applies.

Appendix A – Useful Definitions

Personal data

Data that relates to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Special category data

Special category data are subject to stricter conditions when processing. These are details about an individual's:

- Race;
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetics
- Biometrics (where used for ID purposes)
- Health (physical or mental)
- Sex life
- Sexual orientation

Data Controller

Any person or organisation who (either alone, jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. The GMC is a Data Controller.

Data Subject

An identifiable natural person who can be identified directly or indirectly

Processing

Any handling of personal data. This includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Data Processor

Any person or organisation who processes personal information on behalf of the Data Controller