Data Protection Policy

Contents

Introduction

The UK General Data Protection Regulation 2016 (UK GDPR) and the Data Protection Act 2018 (DPA) impose certain obligations on data controllers who process personal data.

The Health & Care Professions Council (HCPC) is a data controller as defined by the UK GDPR and DPA. We need to collect and use personal data to carry out our statutory responsibilities under the Health Professions Order 2001. We hold personal information about our registrants, but we also hold information about others. This includes those who raise concerns about our registrants, current, past and prospective employees, our Partners and Council members.

All personal information must be collected, used, stored and disposed of properly and in accordance with the principles of the UK GDPR and the DPA.

Purpose and Scope

The purpose of this policy is to set out the HCPC approach to handling personal data and our obligations as set out in the UK GDPR and DPA.

This policy applies to:

- all HCPC employees, temporary staff (such as agency and interim workers), Council Members, Partners, contractors and other authorised users of HCPC information systems.
- personal data as defined by Article 4 of the UK GDPR; that is any information relating to an identified or identifiable natural person.
- 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 and ethnic origin) and data relating to criminal convictions and offences as defined by Article 10 of the UK GDPR. Special category personal data and criminal convictions data is data that is particularly sensitive and therefore attracts specific protection.

Responsibilities

Information Governance team

The Information Governance team will provide advice, guidance and training to staff to ensure consistency in the handling of personal data. The team will also be responsible for processing individual rights requests introduced by the UK GDPR.

Information Security Group (acts as the Information Security Management System (ISMS) Board)

The ISMS Board supports the information security management framework in operation from ISO27001. The key responsibilities of the Board include:

- approving and supporting the Information Security Management System
- developing, supporting and implementing the HCPC information security policies and procedures
- supporting the Chief Information Security & Risk Officer for coordinating the implementation of information security and business continuity management
- reviewing and monitoring data incident reports together with the results of any investigation carried out
- recommending changes to other policies and procedures based on security incidents and changes in risks

Data Protection Officer (DPO)

The DPO has operational responsibility for data protection at the HCPC. As set out in Article 39 of the UK GDPR, the functions of the DPO are to be involved on a day-to-day basis in data protection compliance.

Partners

Partners are HCPC registrants, members of the public and legal professionals who contribute their expertise to the HCPC and play important roles in the regulatory process. They provide the expertise the HCPC needs for its decision making processes and ensure that we have good professional and lay (public) input into what we do.

The HCPC will provide guidance and training to Partners to make them aware of how they can comply with data protection legislation while they work with or for us.

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

All Staff and Contractors

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 information security eLearning training within the requisite timeframe.

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

Policy

Data protection principles

The UK General Data Protection Regulation 2016 (UK GDPR) and Data Protection Act 2018 (DPA) aim to strike a balance between the privacy rights of individuals and the ability of organisations to process personal information in the course of legitimate business.

Data protection legislation stipulates how we collect and process personal data in a lawful way, which is fair to the individuals the information is about (data subjects) and meets their reasonable expectations.

The principles set out in Article 5 of the UK GDPR and Part 3, Chapter 2 of the DPA apply to this policy. When we process personal information, we will comply with the data protection principles. These are that personal data must be:

Principle 1: processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

Principle 2: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

Principle 3: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Principle 4: 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');

Principle 5: 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 ('storage limitation');

Principle 6: 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).

The HCPC, as a data controller is responsible for and must be able to demonstrate compliance with the six data protection principles

Data subject rights

A data subject has certain rights under data protection legislation:

- **to be informed** - the right to be informed about the collection and use of their personal data.
- **of access** – the right to access their personal data. The right of access allows individuals to be aware of and verify the lawfulness of processing.
- **to rectification** – the right to have inaccurate personal data rectified, or completed if it is incomplete.
- **to erasure** – the right to have personal data erased. The right is not absolute and only applies in certain circumstances.
- **to restrict processing** – the right to request the restrict ion or suppression of their personal data. The right is not absolute and only applies in certain circumstances.
- **to data portability** – the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- **to object** – the right to object to processing based on the legitimate interests or performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processes for purposes of scientific/historical research and statistics.
- **in relation to automated decision making and profiling** – the right to be provided with information about automated individual decision-making, including profiling.

An individual may make a request under any of these rights and the HCPC 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.

All requests to invoke the above rights must be sent either by email to foi@hcpc-uk.org or by post to the Information Governance team, so that the request can be processed.

Subject access requests

We will process subject access requests (SAR) in line with data protection legislation.

Data subjects have the right, upon request, to be informed whether or not information about them is being processed by us, to be given a description of the information, the purpose of our processing and to whom it may be disclosed and to be provided with the information we hold in an intelligible form.

Employees and those working on our behalf must be trained to recognise these requests for information, as the request will not necessarily be labelled under the correct legislation and does not require to be specifically headed as a SAR.

The Information Governance team manages SARs received and all requests must be sent either by email to foi@hcpc-uk.org or by post to the Information Governance team.

Security

As required by the UK GDPR 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 unintended destruction, loss, unauthorised access and disclosure.

Access to personal information will be restricted to those who need to access it and have the right to access it.

Transfer of personal data

We will always seek written consent from the data subject before sending any personal information outside of the European Economic Area (EEA). Unless we are required to do so as part of our regulatory responsibilities, we are confident it is in the public interest and otherwise where it is adequately protected.

Data security incidents

The HCPC 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 is a reported concern about the use, access and destruction of personal data. All incidents should be reported to the Information Governance team as soon as we become aware of them so that we can investigate and take action to limit their impact.

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

Employees, contractors, Partners, Council Members and HCPC data processors should contact the Information Governance team immediately they become aware of a data breach by email to informationsecurity@hcpc-uk.org. An information incident report should be completed.

Data protection impact assessments

Data protection impact assessments (DPIAs) help us think about any privacy and confidentiality issues before the start of a new project or initiative. DPIAs allow us to identify potential risks and to develop a plan to manage and mitigate them. DPIAs help to ensure that we are compliant with data protection legislation.

The UK GDPR introduces a mandatory DPIA requirement for projects which, for example, introduce new technology or involve high risk personal data processing.

Appendix A – Useful Definitions

Personal Data	Any information relating to an identified or identifiable natural person who can be directly or indirectly identified by that data or that data combined with other data.
Special Category Personal Data	Special category data is personal data which the UK GDPR says is more sensitive, and so needs more protection. 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 Subject	An individual who is the subject of personal data who can be identified directly or indirectly.
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, processes. The HCPC is a data controller.
Data Processor	Any person or organisation who processes personal information on behalf of the Data Controller according to clear instructions. They are not able to use the data for any other purpose.
Processing	Almost anything you do to personal data can be called processing. This includes any operation or set of operations which is performed on personal data or sets of personal data whether or not by automated means. This includes collection, recording, storing, sharing, amending or destroying data.
Data Protection Officer	A Data Protection Officer is the lead for Data Protection within an organisation. They have specialist knowledge and act as a source of advice on Data Protection issues.
Data Protection Act 2018 (DPA)	The Data Protection Act 2018 is the UK's implementation of the EU GDPR in primary legislation. It sits alongside and supplements the UK GDPR for example by providing exemptions.
UK General Data Protection Regulations (UK GDPR)	The UK General Data Protection Regulation (UK GDPR) is a legal framework that sets rules for the collection and processing of personal information of individuals within the UK. It came into effect on 1 January 2021 and is based on the EU GDPR.

Information Commissioner's Office (ICO)	The ICO is the UK regulator of Data Protection rights. Individuals can contact them if they have concerns about how their personal data is being used or how their information rights have been respected. The ICO also regulates access to public information (Freedom of Information).

V1.0
15 January 2026