Information Governance Policy

V6.0

Document Information

Title of document	Information Governance Policy

Document Control

Version Number	Reason for Change	Description of Change	Date of Change	Author
v1.0	New document	New document		

Check the policies section of the

1. Introduction

The Royal College of Psychiatrists (the College) is the professional medical body responsible for supporting psychiatrists throughout their careers, from training through to retirement, and in setting and raising standards of psychiatry in the United Kingdom. The College holds and manages personal and confidential information relating to psychiatrists, College staff, experts,

	requirements under data protection law and for ensuring they comply with these on a daily basis and ensure that no breaches of information security or confidentiality result from their actions. Should any staff action(s) result in a breach it must be reported to the DPO within 24 hours. All staff shall be responsible for the operational security of the information systems they access and use. All staff are required to undertake mandatory information governance training covering GDPR, confidentiality and information security.

5. Governance Structure

The Data Protection Leads Group provides assurance that the organisation is compliant with information legislation and that all information is managed in accordance with the privacy principles, Caldicott Principles (in the case of patient/service user data), GDPR, Data Protection Act 2018 and other relevant legislation. The IG Framework at Appendix B gives more detail on this.

6. Definitions

Term	Definition
Access to Health Records Act 1990	Provides controls on the management and disclosure of health records for deceased individuals. The personal representative of the deceased or a person who might have a claim arising from the individual's death can apply to request access to the files.
Archive	Those records that are appraised as having permanent value.
Audit (Records)	A planned and documented activity to determine by investigation, examination or evaluation of objective evidence, the adequacy and compliance with established procedures, or applicable documents, and the effectiveness of implementation.
Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient/service user information and enabling appropriate information sharing.
Common law	The law

	it is reasonable to expect that the information will be held in confidence.
Consent	An agreement that

	eventual disposal, according to their administrative, legal, and/or financial evaluation.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. E.g. A request is received on 30 January. The response date cannot be 30 February as there are not enough days in the month so the response date is 28 February (except in a leap year when it would be the 29th).

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Staff who receive a subject access request from a patient or carer must take the details of the information required and contact details of the requestor and pass them to the Data Protection Officer (DPO) for processing. The information can be emailed to: dataprotection@rcpsych.ac.uk.

12. Record Keeping

Record keeping and records management is an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the company and preserving an appropriate historical record. Examples of the key components of records management include creation, storage, transfer, closure, retention, archiving and disposal.

Records and documents are different. Documents consist of information or data that can be structured or unstructured. Records provide evidence of the activities of the College functions and policies. Records have strict compliance requirements regarding their retention, access and destruction, and generally have to be kept unchanged. Conversely, all records are documents.

Audio or video recording of meetings should only be carried out as a backup for minuting purposes. The minutes are the official record of the meeting and as such the recording should be deleted immediately after the minutes relating to the recording have been approved. If inappropriate behaviour is captured in a meeting recording, that recording may be retained under the GDPR legal basis of legitimate interest for the College.

The College Records Management Policy and Records Retention Schedule contain more detail on record keeping and can be found on the Intranet.

13. Information Sharing

Information and data sharing is essential to support and facilitate business processes. Personal identifiable data will only be used for legitimate interests and with a legal basis. Access to personal identifiable data will:

be on a need to know basis;

use only the minimum amount of information required; and

be provided within a secure system.

Personal identifiable data will not be shared or otherwise released unless appropriately authorised. All information sharing must have agreed processes for authorising the use of personal identifiable data. Where there is not an approved process already in place, a Data Protection Impact Assessment must be completed, approved and an agreement signed before any sharing of data