Information Governance Policy

V3.0

Document Information

Title of document	Information Governance Policy
Version number	V3.0
Type of document	Policy
Purpose of document	To provide a framework to ensure compliance with legislation and for the effective management and protection of organisational and personal information.
Target audience	All College staff, contractors, secondees.
Distribution	College intranet (electronic) College Website (electronic)
Consultation	CEO, Director of Finance
Approved by	Calum Mercer, Director of Finance and Operations
Date of approval	June 2019
Author	Richa Kataria, Head of Membership Services and Faculties
Review date	June 2020

Document Control

Version Number	Reason for Change	Description of Change	Date of Change	Author
v1.0	New document	New document	01/06/18	Kathryn Campling
V2.0	Updating document	Updating document	27/09/2018	Kathryn Campling
V3.0	Updating document	Amendments have been made to reflect that the Director of Information Services is responsible for the tasks assigned in the previous version to the Head of IT.	28/05/2019	Richa Kataria

Table of Contents

Appendices

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, members of the public and patients in varying degrees of detail.

Information is a fundamental asset to the organisation and as such, we need to ensure there are robust arrangements for information governance. It is of paramount importance that information is efficiently managed; that appropriate accountability, standards, policies and procedures provide a robust governance framework for information management.

Information Governance compliance is supported by the key roles of the Chief Executive Officer as Senior Information Risk Officer (SIRO) and the Data Protection Officer. However, all staff have a duty of confidentiality to protect the privacy of information and to help the organisation achieve its strategic objectives.

2. Aims and Objectives

The overall aim of this policy is to ensure that information governance is embedded throughout the organisation and forms an integral part of everyday practice within each directorate. This is achieved by ensuring that a cohesive and comprehensive information governance framework is in place with clearly defined responsibilities in order to support the organisation in delivering services, ensuring compliance with information legislation and establishing a robust governance framework (see appendix B) for information management for preserving the confidentiality, integrity, security and accessibility of data, processing systems and information within the College This policy also helps ensure that the organisation can achieve its strategic and operational objectives.

Aims

- Comply with legal and contractual obligations and meet the requirements of funders (for example in the case of CCQI and NCCMH), external regulators and other relevant bodies
- Ensure the Board of Trustees are provided with accurate and relevant information regarding the organisation's compliance with information legislation and best practice to better inform policy and decision making
- Provide assurance that continuous improvement through the effective use of information are integral to the activities of the organisation

Objectives

- Integrate information governance into the organisational culture and everyday practice

- Ensure a standard information governance framework is adopted by all directorates.
- Demonstrate the organisation's approach and commitment to information governance and data protection
- Encourage and support the reporting of information related incidents (e.g. breaches, losses of information) within an open, fair and just culture by providing training and feedback to staff
- Maintain a documentation and record keeping audit regime for all services
- Ensure all staff are aware of their obligations regarding information governance

3. Scope

This policy applies to all staff employed by the College regardless of their job role, length of service, seniority, type of employment, length of contract, place of employment or the service they are employed in. This policy also applies to all work-related activities regardless of the actual location (i.e. staff working from home, a private or company vehicle in transit, an external venue or another organisation's premises).

This policy will be applied fairly and consistently to all employees regardless of their protected characteristics as defined by the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation).

This policy also applies to those Members who are not employed by the College but work on Faculties, papers, Committees and other College business.

The organisation will also make reasonable adjustments to the processes within this policy so as not to disadvantage any employees with disabilities. Any employee who has difficulty in communicating, verbally or in writing, will have arrangements put in place as necessary to ensure that this policy and the processes within are understood and that the employee is not disadvantaged in any way.

The principles within this policy are primarily aimed at the use of personal data but can be applied to commercially sensitive business data also.

4. Duties and responsibilities

Senior Management Team (SMT)	• It is the role of the SMT to define the organisation's policy in respect of Information Governance and risk and meeting legal and statutory requirements. • They are responsible for ensuring sufficient resources are provided to support the requirement of this policy. • The responsibility of this is delegated through the CEO as Senior Information Risk Owner (SIRO) • The SMT will receive exception reports on information governance and data protection issues and this will be completed through the Data Protection Leads Group.

Senior Information Risk Owner (SIRO)	• The CEO is SIRO and is responsible for the management and mitigation of information management process risks. • SIRO will act as advocate for information governance risk(s) at Senior Management Team.
Data Protection Officer	• The Data Protection Officer (DPO) provides independent advice to support the organisation's decision making in the appropriateness of processing personal and special categories of data within the principles and rights of the General Data Protection Regulation (GDPR) and Data Protection Act 2018. • The DPO will develop and provide suitable information governance training and e-learning training updates for all staff. • Monitors actual or potential reported information security incidents reported across the organisation. • Supports and assists the Head of IT with regard to information security incidents. • Raise awareness of information governance within the organisation as part of business as usual activity. • Provide quarterly and annual updates on information governance assurance to the Information Governance Group and will report on an exception basis on information governance issues and risks.
Director of Information Services	• The Director of Information Services provides expert technical advice to the organisation on matters relating to IT security and ensuring compliance. • Acts as the organisation's IT Security Manager. • Works collaboratively with the DPO and SIRO with regard to information security incidents.
Data Protection Leads	• Data Protection Leads (DPL) are responsible for ensuring that the policy and its supporting standards and guidelines are enshrined into local processes and that there is ongoing compliance. • DPL ensure that all staff undertake mandatory information governance training and that ongoing training needs are routinely assessed. • DPL shall be individually responsible for the security of their physical environment where information is processed and stored. • DPL will support the DPO in the investigation of any breaches.

All staff	• All staff (temporary and permanent) and contractors are responsible for ensuring they are aware of their 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 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 implantation.
Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient/service user information and enabling appropriate information sharing.
Common law	The law derived from decisions from the courts, rather than Acts of Parliament or other legislation.

Confidentiality	A duty of confidence arises when one person discloses information to another (e.g. service user to clinician), in circumstances where it is reasonable to expect that the information will be held in confidence.
Consent	An agreement that is freely given, specific, informed and an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of their personal data.
Data controller	A person who (either alone or 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.
Data processor	Any person (other than an employee of the data controller) who processed the data on behalf of the data controller.
Data Protection Act 2018	A revised Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information. The Act sits alongside the GDPR.
Data quality	This refers to the procedures and processes in place to ensure that data is accurate, up-to-date, free from duplication (e.g. where two or more different records exist for the same individual), and free from confusion - where different parts of an individual's records are held in different places, and possibly in different formats.
Data subject	An individual who is the subject of personal data.
Disclosure	The divulging or provision of access to data.
Disposal	The implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example paper to electronic and/or vice versa).
Encryption	Encryption is the means of converting information using a code that prevents it being understood by anyone who isn't authorised to read it.
Freedom of Information Act 2000	This requires all public authorities to make certain information available to the public either through regular publication or on request.
GDPR	The General Data Protection Regulation is an EU regulation on data protection and privacy for all individuals. It aims to give control

	to individuals over their personal data with enhance rights over previous information legislation. The GDPR sits alongside the Data Protection Act 2018.
Information	Includes information in any media (Including paper records and electronic data, clinical records, letters, emails, CDs, DVDs, patient administration systems, corporate information including staff records, financial records and estates and facilities).
Information asset(s)	Includes operating systems, infrastructure, business applications, off the shelf products, services and user developed applications.
Data Protection Leads	Data Protection Leads (DP leads) are directly accountable to the Senior Information Risk Owner (SIRO) for the tasks relating to their role and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. In this regard, DP leads may be assigned ownership of several assets of their organisation that may include components reused in assets of other DP leads (e.g. hardware and software).
Information asset register	A list of the assets the College relies on in order to carry out its day-to-day business. See also information asset.
Information Commissioner	The Information Commissioner (ICO) is the UK's independent authority to uphold information rights.
Information governance	A set of multi-disciplinary structures, policies, procedures, processes and controls required to manage information in support of an organisation's regulatory, legal, risk, environmental and operational requirements. It allows organisations and individuals to ensure information is processed legally, securely, efficiently and effectively.
NHS number	The NHS number is a unique 10 character number assigned to every individual registered with the NHS in England and Wales. The NHS number is used as the common identifier for patients across different NHS organisations.
Personal information	Also referred to as "personal identifiable information" (PID) and relates to information about a person which enables that person's identity to be established by one means or another.
Record	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business.

Retention	The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their eventual disposal, according to their administrative, legal, and/or financial evaluation.
Safe haven	The term used to explain an agreed set of arrangements that are in place in an organisation to ensure person identifiable, confidential and/or sensitive information can be received, stored and communicated safely and securely.
Sensitive information	Special categories of personal data including genetic data, biometric data, racial or ethnic origin and data concerning health. A category of personal information whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community.
Subject Access Request (SAR)	A request from an individual to see information held on them. This request can be made in writing or verbally.

7. GDPR and Data Protection Act 2018

The Data Protection Act 1998 has been repealed and replaced by the GDPR and the Data Protection Act 2018. The new regulation and legislation enhances privacy rights and rights of individuals' where their personal data is concerned.

Within the new legislation there are six principles relating to the processing of personal data.

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('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 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('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').

8. Rights of the data subject

Under the GDPR and DPA, data subjects have certain rights, which must be upheld. These include:

- Be informed which is processed through privacy notices and Data Protection Impact Assessments;
- Access to their own personal data through subject access requests;
- Rectification; which is having inaccuracies corrected;
- Erasure, or right to be forgotten, which is the right to have information erased. Should an individual make a request to prevent processing then depending on the individual circumstances, we would have to make a judgement based on the risk(s) to the individual, or others, whether it was right to provide a service. This decision will be made by the SIRO and DPO;
- Object to processing, for example direct marketing.
- Prevent automated decision-making and profiling;
- Data portability; which is having information provided in electronic format and not hinder the data subject's transmission of personal data to a new data controller; and
- Consent to process. Silence, pre-ticked boxes or inactivity does not constitute consent to process under the new rules.

9. Freedom of Information Act 2000

The College does not fall under the scope of the Freedom of Information Act 2000 as it is not defined as a public authority under section 3 of the Act. However, requests for information about the College could be made to our funders and it may be necessary to either confirm or deny whether the information requested is held. To that end, a summary of the requirements to ensure compliance with the Act is detailed here.

The Freedom of Information Act 2000 gives anyone the right to make a written request (including an e-mail request) to see information held by public authorities. The Act only concerns information that is 'held' by an organisation. By held this means recorded, either electronically or in hard copy format. If the information is held, it will usually be disclosed. Any information can be requested, no matter how old it may be. This includes reports, minutes of meetings, activity data, financial data, information contained within emails or correspondence etc. There are only a small number of exemptions provided for under the Act which allow organisations to withhold information. An example of this would be personal or commercially sensitive information.

Requests do not have to specifically mention the Act, nor do they have to state why the applicant requires the information. Organisations must respond to requests for information within 20 working days and if it does not, it may be liable for penalties.

If someone asks you for information that you have to hand or normally give out (e.g. an information leaflet, routine letter, newsletter etc.), you should continue to do so. These requests do not need to be logged or dealt with under the Act.

If you have been contacted by someone requesting information under the Freedom of Information Act 2000, you should direct them to the DPO:

- E-mail: dataprotection@rcpsych.ac.uk

Please also be mindful that deleting or destroying information after a request has been made under the Act is likely to be viewed as a criminal offence. To delete and/or destroy information in this way will also be considered to be gross misconduct under the company's disciplinary process.

10. Pseudonymisation of Identifiable Data

Personal data that has been pseudonymised, for example key-coded, can fall within the scope of information legislation depending on how difficult it is to attribute the pseudonym to a particular individual. Pseudonymisation is the process of distinguishing identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know identity. Pseudonymised data is still personal data and should be afforded that same protection.

We must ensure appropriate changes are made to processes, systems and security mechanisms in order to facilitate the use of de-identified data in place of identifiable data where appropriate.

Personal information that we hold includes any confidential information which identifies a living individual. This may thereby breach their right to privacy or present a risk of identity theft if lost or inappropriately shared. This applies to data relating to service users, staff and any other parties. It does not apply to identifiable data already in the public domain.

11. Subject Access Requests

The right of access, also known as a subject access request, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. Subject access requests are processed under the GDPR and Data Protection Act 2018. The College must comply with the request and respond promptly within one month.

Subject access requests must be made either verbally or in writing. It can also be made to any part of the organisation including social media and does not have to be to a specific person or point of contact.

Depending on the information requested, staff may be required to assist in the collation of information, including emails, electronic and hard-copy records.

The time limit for the request is one calendar month. The calculation starts the day after receipt of the request and ends on the corresponding day in the following month. E.g. a request is received on the 3rd October. The calculation starts on the 4th October and the request must be responded to by the 4th of November.

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 the 30 January. The response date cannot be the 30 February as there are not enough days in the month so the response date is the 28th 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 service user must take the details of the information required, 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.

The College Records Management Policy contains more detail and can be found on the Intranet.

13. Information Sharing

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

- On a need to know basis;
- Use only the minimum amount of information required; and
- 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 person 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 commences. Should any personal identifiable or sensitive data be unintentionally received by a member of staff, the Data Protection Officer must be contacted and the sender must be advised that they have incorrectly shared identifiable or sensitive data,

an incident report should be completed and that they should review their local policies and procedures to ensure it does not happen again.

Security measure such as password protection and/or encryption should be used for transporting personal data in electronic forms.

14. Training Requirements

It is essential that all staff receive information governance training. All new staff will receive information governance training as part of their induction process within the first few weeks of starting with the College. All current staff receive refresher training every 2 years.

15. Associated Documents

Subject access request procedure

IT security policy

Privacy Notices (various)

16. Review and monitoring

This policy will be reviewed in May 2019 following the introduction of the GDPR and DPA in May 2018.

Appendices

Appendix A: Key information governance contacts

Appendix B: Information governance framework

Appendix A: Key Information Governance Contacts

In the first instance, should you have any information governance related queries please speak to your line manager.

Day to day information governance and data protection / confidentiality queries

Data Protection Officer

E-mail: dataprotection@rcpsych.ac.uk

Senior Information Risk Owner (SIRO)

CEO

Tel. 020 3701 2589

E-mail: paul.rees@rcpsych.ac.uk

IT

Chris Lord, Head of IT

Tel. 0207 3701 2585

E-mail: chris.lord@rcpsych.ac.uk

If there has been a loss of information or a breach of confidentiality, immediately report this to the DPO using dataprotection@rcpsych.ac.uk and notify your Data Protection Lead.

Appendix B: Information Governance Framework

This Information Governance Framework document aims to capture the Royal College of Psychiatrist's approach to information governance.

Robust Information Governance (IG) requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. This strategy must be read in conjunction with the organisation's Information Governance Policy.

Through the implementation of this policy, we will:

1. establish robust information governance processes conforming with legislation, best practice and national standards;

2. ensure that clear information is given about how personal information is recorded, handled, stored and, where required, shared by the organisation. The public will be provided with guidance to explain their rights, how their information is handled, how they can obtain further information and how they can raise concerns. This is published in the privacy notices which are available on the public website;

3. provide clear advice and guidance to staff and ensure that they understand and apply the principles of information governance to their working practices as business as usual;

4. ensure that procedures are reviewed on a regular basis to monitor their effectiveness in order that improvements or deficiencies in information handling standards can be recognised and addressed;

5. work to embed and enshrine an open information governance culture within the organisation through increasing awareness and providing training on the key issues;

6. maintain a clear reporting structure and ensure that through management action and training all staff understand the requirements of information governance and their responsibilities;

7. undertake regular reviews and audits of how information is recorded, held and used which will inform best practice;

8. ensure that there are robust procedures for notifying and learning from IG breaches and incidents in line with the Incident Reporting Process;

This work is monitored, reviewed and signed off by the Data Protection Leads Group.