DATA PROTECTION POLICY AND PROCEDURES 2024

Working together to handle personal data safely, respectfully and lawfully

Document Control

Author:	**Head of Information and Governance**	**Accountable Executive Director:**	**Membership, Global and Governance**
Version:	**2024**	**Last review date:**	**2023**
Approving body:	**Executive Committee**	**Date of approval:**	May 2024
Related policies:	Privacy Policy 2024, DSP Incident Handling Policy 2024 and Records Management Policy 2024, IT Security Policy 2022, Special Category Data Policy 2023, BYOD Policy 2022	**Date of next review:**	January-March 2025

Document revision history

Version	Date	Author	Summary of changes
2019	31 March 2019	Head of Information and Governance	Universal policy for all employees, officers and individuals/organisations processing personal data on behalf of the RCOG
2020	07 July 2020	Head of Information and Governance	New Special Category Personal Data policy and handling requirements; new DSP controls re: health and care data
2022	21 September 2021-28 January 2022	Head of Information and Governance	Re-formatted; new College roles in scope; clarification re: definition of employees; new DSP Toolkit requirements; aligned to the Digital Social Care template; new policy waiver form/approval process; and a more comprehensive Procedures section
2023	February 2023	Head of Information and Governance	New section on international transfer; changes to the DPIA template and process; and a streamlining of the SCD

			policy requirements; SCD policy published separately
2024	March 2024	Head of Information and Governance	Inserted examples of contracts

Data Protection: Policy on a Page

What is personal data?

"Data which relates to a living, identifiable individual, that is biographical in nature and has them as its focus" – an 'identifier'.

What does data protection mean: busting the jargon?

In plain English, you should only use personal data you are allowed to, be transparent (a), and use it for a specific purpose (b) then…

- only collect what you need (c)
- keep it accurate and up to date (d)
- get rid of it when you no longer need it (e)
- keep it safe and protect it from wrongful use (f)
- be accountable and document how we use it (g).

What are the reasons for processing information?

There are **6 lawful bases for processing** personal data, the College uses the following **3**:

- **Legitimate interests**
- **Contract**
- **Consent.**

What rights do individuals have?

1. the right to be **informed**
2. the right of **access**
3. the right to **rectification**
4. the right to **erasure**
5. the right to **restrict processing**
6. the right to **data portability**
7. the right to **object**
8. rights in relation to **automated decision making and profiling.**

What does it mean for me?

- **All employees, Trainees, members, Officers, Board of Trustees/Committee members, volunteers, College representatives and suppliers:**
  - Must **complete induction, refresher and specific training**, appropriate to their role/to the College's standards
  - Must **follow all data protection requirements in their respective role descriptions, contracts, terms and conditions and/or Code of Conduct**
  - Must **inform the IG Team of any Individual Rights Request** received relating to the College
  - Must **protect and secure all handling of personal data – e.g.**
    - **Encrypt the transfers of personal data**
    - **Only use College devices and tools** to store and process personal data
    - **Follow the College's security rules,** such as wearing your ID badge
    - **Follow the Agile Working Guidance** with particular regard to the handling of paper records and not using personal devices/webmail to process College information
    - **Avoid the inappropriate copying, downloading or sharing of any personal data**
    - **Use confidential waste for the disposal of all sensitive and personal data**
  - Must **complete full contractual due diligence on all new or renewed contracts**
  - Must **ensure there is a lawful basis of processing** in place before handling any personal data
  - Must **promptly report potential or actual breaches of the Policy or data protection law**.
- **All employees** :
  - **Processing special category personal data** or with a dedicated IG role **must attend the Advanced Data Protection training or equivalent**
  - Must **assess and manage the risks** around how they process personal data using DPIAs
  - Must **manage College records containing personal data** in compliance with the RCOG Retention Schedule
  - Must **maintain the departmental sections of the Record of Processing Activity** in the RCOG Information Asset Register.

The College will take appropriate action against employees, officers, trainees, members, College representatives or suppliers found breaching the Policy where appropriate to them.

Contents

Introduction

This Data Protection Policy is the Royal College of Obstetricians and Gynaecologists' (RCOG or the College) policy regarding the safekeeping of all the personal data processed to deliver the College's business.

In order to conduct its normal business, the College collects and uses certain types of personal information about living individuals. These include current, past and prospective trainees, members, employees, College representatives, suppliers, clients, customers, and others with whom it has business, or with whom it communicates. We will be open and transparent with all our data subjects, from members of employees to RCOG fellows.

The College considers the lawful and correct treatment of such personal information as essential to the efficient and successful conduct of its business. It also recognises that it is crucial to fostering and maintaining the confidence of its main stakeholders and the wider public in the College and its operations.

Purpose

The purpose of the Royal College of Obstetricians and Gynaecologists (RCOG or the College) Data Protection Policy is to:

- comply with Data Protection Law and the common law of confidentiality, e.g. data protection impact assessments and the Caldicott Principles, and all other relevant national legislation
- support the 10 Data Security Standards, e.g. the NHS Data Security and Protection Toolkit
- meet our data protection standards, e.g. information sharing arrangements
- protect the rights of our employees, officers, trainees, members, College representatives, suppliers, clients, customers and public users, e.g. procedures to govern Individual Rights' request handling
- protect the College from the risks of a data protection breach and related reputational, financial and legal damage, e.g. encrypt special category personal data.

Data Protection Law, namely UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018, set out the framework for how the UK processes personal data:

- UK GDPR, enforceable from January 2020, covers most of the legal obligations for processing personal data in the UK
- DPA enacts GDPR and replaces the DPA 1998. It sets out:
    - how other information rights legislation (e.g. Freedom of Information Act 2000) interact with the new DPA and GDPR
    - local rules that complement UK GDPR, e.g. additional measures required for the processing of special category personal data
    - the Information Commissioner's Office's (ICO) role, functions and powers.

This policy covers:

- Our data protection principles and commitment to common law and legislative compliance
- Procedures for data protection by design and by default.

It is underpinned by the following specific policies and procedures:

- Agile Working Guidance (internal only)
- NHS Data Security and Protection Toolkit – Category 3
- Contract Signing Policy (internal only)
- Data Security and Protection Incident Handling Policy and Procedures
- IT Security Policy (internal only)
- Privacy Policy
- Records Management Policy and Procedures, including our Data Quality standards.

Scope

The Policy applies to:

- **all employees (permanent, temporary, contracted and voluntary), officers, Board of Trustee/Committee members, trainees, members, College representatives and suppliers** who handle and use our information (where we're the 'Controller' for the personal data being processed), whether we hold it on our systems (manual and automated) or if others hold it on their systems for us
- **all personal data processing** we carry out for others (where we're the 'Processor' for the personal data being processed)
- **all formats of personal data**, e.g. printed and digital information, text and images, documents and records, data and audio recordings

Policy

The RCOG takes data protection seriously and adheres to UK data protection law governing the collection and management of personal information.

Personal data is all information that relates to an identifiable living person (or "Data Subject") **and** that can be used to identify the person directly, or indirectly when used with other information. It includes but is not limited to:

- a person's name
- job title
- age
- postal or email address
- IP address, e.g. online identifier
- vehicle registration number
- bank details
- in addition, any other information that relates to them, e.g. a pseudonym such as a National Training, NHS or hospital number.

We use personal data to fulfil our regulatory and statutory obligations, establish professional expertise and status, as well as to confirm identities for legal or regulatory purposes. We also use the information provided by individuals to deliver the tailored services and benefits of the RCOG membership package and/or O&G specialist-training programme. These services include:

- Receiving the latest news and developments in O&G
- Educational opportunities like eLearning resources, courses and events
- Update on College activities and opportunities to get involved

- Access to the CPD and/or Training ePortfolio
- New and revised clinical guidance and techniques
- Insight into new journal and research content.

The College reserves the right to take appropriate action against employees, officers, trainees, members, College representatives or suppliers found to be in breach of the Policy, or any other College ~~P~~olicy or third party agreement including but not limited to Codes of Conduct, Confidentiality and Non-Disclosure Agreements.

Principles

We ensure our processing of personal data complies with the following data protection principles:

a) Be processed lawfully, fairly and in a transparent manner (**Lawful, fair and transparent**) – e.g. establish, maintain and publish policies to ensure controlled and appropriate sharing of personal data with legitimate third parties, taking account of all relevant legislation and consent
b) Be obtained only for specific, lawful purposes (**Purpose limitation**)
c) Be adequate, relevant and limited to what is necessary (**Data minimisation**)
d) Be accurate and, where necessary, kept up to date (**Accuracy**)
e) Not be held for any longer than necessary (**Storage limitation**)
f) Be protected in appropriate ways (Integrity and confidentiality/**Security**)

Lawful Basis

All personal data processing must have a **lawful basis for processing** from the following:

- the Data Subject (see Roles and Responsibilities below) **consents** to the processing of their personal data
- the processing is necessary:
    - to enter into or carry out a **contract** with the Data Subject
    - to comply with our **legal obligations**
    - to protect the **vital interests** of the Data Subject
    - to exercise our official authority or perform a **public interest task**
    - to meet the **legitimate interests** of a Controller (see Roles and Responsibilities below) or another third party.

The College uses the following three legal bases, which determine which of the College's procedures, and ways of working, must be adopted:

- **contract** – where this applies, the contracts must:
    - be written
    - include/based the College's mandatory data protection clauses and schedules whether we are the Client or the Contractor
    - be monitored for compliance
    - be up-to-date.
- **legitimate interests** – where this applies, the Data Subject must be notified using either the College's Privacy Policy and/or a supplementary notification using the College's Privacy Checklist (internal only)
- **consent** – where this applies, the Data Subject must provide explicit and informed consent, which is then managed to enable them to withdraw consent at any time. Please see our Records Management Policy and Procedures for our Withdrawal of Consent procedures.

We meet the following **additional lawful bases** where we process special categories of personal data as defined by GDPR and the DPA:

a) the data subject has given **explicit consent**

b) processing is necessary for the purposes of carrying out the **obligations** and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
d) processing is carried out in the course of its **legitimate** activities with appropriate safeguards by specific organisations, on condition that the processing relates solely to the members or to former members of that organisation
e) processing relates to personal data made **public** by the data subject
f) processing is necessary for the establishment, exercise or defence of **legal claims**
g) processing is necessary for reasons of substantial **public interest**
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of **health** or social care or treatment or the management of health or social care systems and services
i) processing is necessary for reasons of public interest in the area of public health
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical.

Individual Rights

The College commits to processing personal data in compliance with Data Subjects' **Individual Rights**.

Data Subjects have:

1) the right to be **informed** - e.g. fair processing/privacy notices
2) the right of **access** - e.g. subject access requests (SARs)
3) the right to **rectification** - e.g. have their data corrected
4) the right to **erasure** – e.g. have their data deleted/removed
5) the right to **restrict processing** – e.g. stop their data being used
6) the right to **data portability** – e.g. transfer their data easily
7) the right to **object** – e.g. challenge what we're doing with their data
8) rights in relation to **automated decision making and profiling** – e.g. safeguards to make sure we do not make potentially damaging decisions about them without human involvement.

As part of these rights, Data Subjects can:

- make a verbal request against any of the rights listed above; and
- complain to the ICO about data protection breaches and can bring court proceedings for compensation where a data protection breach has caused them damage (including distress).

Special Category Data

The Special Categories of personal data and these include but not limited to data revealing:

- race or ethnicity
- religious or philosophical beliefs
- trade union membership
- a person's health
- sex life or sexual orientation
- genetic or biometric data.

The College applies additional controls when processing special categories personal data (SCPD) in order to retain compliance with the UK Data Protection Act 2018 – please see Principles above. In summary:

- Schedule 1: condition for processing
- The application of additional lawful bases (see above)
- Additional procedures for ensuring compliance with the principles (see Procedures below)
- Additional IT security controls (see Procedures below).

Data Protection by Design and by Default

The College implements appropriate organisational and technical measures to uphold the principles outlined above using a Data Protection Impact Assessment (DPIA) template. All new/upgrades/renewals of contracts, projects, procurements, and initiatives must complete the DPIA's Screening Questions to assess the level of risk and whether the full DPIA needs to be completed. This ensures we:

- integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing
- uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process
- assess whether we should complete a Data Protection Impact Assessment (DPIA), prior to starting any new data processing by completing Step One of the RCOG DPIA
- build data protection from the beginning of the system change
- record, risk assess and maintain our processing into the RCOG Information Asset Register and Records of Processing Activities
- ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks by completing the RCOG DPIA
- Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

Contract Procurement and Management

Contract procurement and management – all contracts where personal data is either stored or processed on behalf of RCOG must:

- complete the DPIA screening questions, and the full DPIA if the data or processing is "high risk"
- use the College's Data Protection Schedule in the first instance or risk assess the equivalent, as per the DPIA
- complete IG contractual due diligence, as per the DPIA.

Information Sharing

All sharing of personal data between Data Controllers must use the RCOG Information Sharing Agreement template or equivalent.

International Transfers of Personal Data

The transfer of personal data outside the UK is referred to as a 'restricted transfer'. These restrictions apply to all transfers, no matter the size of transfer or how often you carry them out.

The College does not transfer personal data to organisations located outside of the UK, unless the rights of the individuals, in respect of their personal data, is protected in another way (e.g. by adequacy regulations or additional safeguards), or one of a limited number of exceptions applies.

In the absence of an adequacy decision, the College complies with UK GDPR rules on restricted transfers by using an Article 46 transfer mechanism as an 'appropriate safeguards', i.e. use of an

International Data Transfer Agreement (IDTA) or Addendum to existing EU GDPR Standard Contractual Clauses (SCCs), further to completing a transfer risk assessment (TRA).

If the outcome of the TRA is that the Article 46 transfer mechanism does not provide the required level of protection, **a transfer must not be made** until extra steps have been taken to ensure that it does.

Learning and Development

The College will provide relevant data protection mandatory induction training and packs; tailored subject specific learning; and communications to employees, Trainees, members, Officers, Board of Trustees/Committee members, volunteers, College representatives and suppliers.

Exemptions

Data protection law exemptions are applied only once they've been considered with reference to the law, ICO issued guidance, the College's other information management and information governance policies and, where appropriate, following guidance from the Research and Information Services Team.

The College reserves the right to investigate and take appropriate action against employees, officers, trainees, members, College representatives or suppliers found to be in breach of the Policy. Such action may include, but not be limited to, disciplinary action up to and including dismissal, civil proceedings and referral to appropriate Regulators.

Procedures

The College commits to processing all personal data in compliance with all the above data protection standards. In summary by:

- **maintaining a** record of our processing activities (**RoPA**), e.g. the College's Information Asset Register
- **appointing a 'Data Protection Officer' (DPO) or equivalent** – the College has less than 250 employees so does not require a DPO therefore the function is shared between the SIRO and Deputy SIRO
- **adopting a 'Privacy by Design and Default' approach** to personal data processing, including completing data protection impact assessments (**DPIA**) on all high-risk data processing, e.g. the College's data protection impact assessment and integration of data protection requirements into all relevant SOPs
- **use the RCOG's Data Protection Schedule in all contracts** involving the storage and/or processing of personal data **and complete the appropriate contractual due diligence** to ensure the suppliers meet our data security and protection standards
- **paying the ICO an annual** data protection fee (**DP Fee**)
- **notifying the ICO within 72 hours** of information security incidents (**IS Incidents**) involving personal data, unless they don't risk data subject's rights and freedoms
- processing personal data within the UK and only transferring it outside the UK if appropriate safeguards are in place, e.g. an adequacy decision
- **implementing sufficient technical controls to enforce this policy**, e.g. to ensure all SCPD is encrypted when "at rest", and to avoid the inappropriate copying, downloading or sharing of any personal data
- **use the RCOG's information sharing agreement template or equivalent** for all sharing of personal data between Data Controllers
- compliance with the **NHS Digital Data Security and Protection Toolkit**

- compliance with the **National Data Opt Out Policy**, e.g. only processing health/patient data where the Data Subjects have not opted out of their data to be used for secondary purposes such as research.

Principles

The College complies with the data protection principles in the following way:

a) **Lawful, fair and transparent**
   - All personal data collected links to the RCOG Privacy Policy to explain the ways we process it, supplementing with specific privacy notices, where appropriate, using our Privacy Checklist – e.g. recruitment
   - Use our Consent Checklist to ensure it is informed, explicit and managed
   - Use the appropriate governance processes outlining roles and responsibilities between data sharing partners to ensure accountability is clearly defined and allocated – e.g. a written contract for suppliers and an ISA for partner data controllers

b) **Purpose limitation**
   - The College only processes personal data in line with the purposes listed in the RCOG Privacy Policy or supplementary privacy notices

c) **Data minimisation**
   - All projects and procurements involving the processing of personal data must complete the RCOG's Data Protection Impact Assessment procedure to ensure only the essential data is collected/created
   - Use codes or pseudonyms instead of names when sharing data with others

d) **Accuracy**
   - The College follows the Data Quality standards outlined in the Records Management Policy and Procedures

e) **Storage limitation**
   - All College records containing personal data are managed in compliance with the RCOG Retention Schedule
   - All College departments maintain their sections of the RCOG Information Asset Register and Record of Processing Activities

f) **Security**
   - The RCOG IT Security Policy informs employees and Officers how to protect and secure all handling of personal data – e.g.
     - Encrypt the transfers of personal data, especially special category data, and obtain Executive Director approval before sharing it
     - Only use College devices and tools to store and process personal data
     - Follow the College's security rules, such as wearing your ID badge, do not access IT server rooms unaccompanied, and be vigilant to individuals in the building without ID badges
     - Follow the Agile Working Guidance with particular regard to the handling of paper records
     - Avoid the inappropriate copying, downloading or sharing of any personal data
     - Ensure all personal devices used for RCOG business comply with the Bring Your Own Device (BYOD) Policy
     - Ensure mobile devices or bags containing personal data are secure when on the move and when agile working – e.g. out of sight in cars, lockable bags/containers and encrypted devices
   - Dispose of all information containing personal and/or confidential data in the Confidential Waste bins throughout the College

- The RCOG Data Protection Impact Assessment procedure ensures all new or upgraded IT systems meet the College's data protection and security standards – e.g. Cyber Essentials Plus certification
- The Data Security and Protection Incident Handling Policy and Procedures ensure all potential breaches of these principles are handled swiftly and lawfully, engaging with the Information Commissioner's Office (ICO) where appropriate – e.g.
    - prompt reporting potential or actual breaches of the Policy or data protection law to the IG Team
    - full co-operation with any investigation, audit or enforcement activity undertaken by the IG Team and ICO.

Lawful Basis

- The Legitimate Interests Assessment procedure must be used by employees when they cite "legitimate interests" as the lawful basis for which they propose to process personal data
- The Data Protection Impact Assessment procedure must be followed for all projects and procurements involving the processing of personal data – this explores all the potential lawful bases and advises which are the most appropriate to apply to the project/procurement

Individual Rights

- The College's Individual Rights Requests guidance advises our membership and public on what they are legally entitled to access, rectify, erase, etc.
- The internal guidance on Handling Requests for Information (RFIs) informs employees and Officers on the College's internal processes for handling Individual Rights Requests – e.g. inform the IG Team of any Individual Rights Request received relating to the College.

Special Category Data

- Those departments processing special categories of personal data (SCPD) where there is a substantial public interest or for an employment, social security and social protection purpose as a Data Controller must implement and maintain the sections of the College Special Category Personal Data Policy tailored to their processing activities This policy ensures compliance with the Data Protection Act 2018, Schedule 1 condition that require the controller to have an **Appropriate Policy Document** in place
- These departments must implement and maintain this tailored policy following completion of the Information Asset Register (IAR) and Record of Processing Activities (ROPA) Update Project in 2023. They will:
    - Attend an SCPD policy and procedures workshop to identify departmental requirements
    - Implement and maintain the relevant sections of the SCPD policy.
- All projects and procurements involving the processing the SCPD must complete a full Data Protection Impact Assessment (DPIA) as such processing is defined by the College as "high" risk – please see Data Protection by Default and by Design below for details.
- Additional IT security controls are required when handling SCPD, including:
    - Data encryption – in transit, at rest and on devices
    - Restricted access servers.

  Details are included in the IT Security Policy.

Data Protection by Design and by Default

Data Protection Impact Assessments (DPIA)

All projects, procurements/contract renewals, procedure reviews and system upgrades ("project") that involve personal data must complete the Screening Questions and Project Description sections of the College's Data Protection Impact Assessment (DPIA).

The Screening Questions have been broken down to enable quick YES/NO responses that determine if the project is HIGH or LOW risk:

- HIGH risk personal data or data processing requires completion of a full DPIA ahead of submission to the IG Team who then propose recommendations to ensure UK GDPR and RCOG IG policy compliance
- LOW risk personal data or data processing requires completion of the Screening Questions and Project Description sections only then submitted to the IG Team who propose standard recommendations which the project is then wholly responsible for implementing and the DPIA is closed.

In the RCOG, HIGH risk...

- data includes:
    - special category data (see above)
    - data of vulnerable data subjects, such as children
- processing involves:
    - storage, transfer, sharing or commissioning of 3rd parties to process personal data outside of the UK (international transfers)
    - systematic monitoring, such as CCTV
    - targeted marketing and fundraising activities
    - large volumes of personal data
    - new, innovative technological solutions
    - matching data from multiple sources, internally or externally
    - prevention of individuals from exercising their rights, such as ability to withdraw consent.

Contract Management

All contracts and service agreements with external third parties (the Contractor or Data Processor) commissioned by the RCOG (the Client or Data Controller) to process personal data on our behalf must be compliant with UK GDPR (see below as to "how") and by following the Contract Signing Policy and completing the Contract Due Diligence Form in order to ensure full due diligence is undertaken by the team managing the contract in partnership with the relevant teams across the College.

Contract examples:

- Software subscription Ts and Cs – e.g. project management tools from 3rd party system suppliers
- Supplier contracts - e.g. media, photocopiers, cleaning, utilities, etc.
- Teaming agreements (where the College agrees in principle to work in partnership with another entity)
- Software Licence Agreements – e.g. online access to licensed e-resources
- Letters of Engagement - e.g. for internal or external audits, or for legal retainers.

All such contractual arrangements must:

- be written

- complete full data protection and security contractual due diligence on all new or renewed contracts that involve the handling of personal data, recommended further to completing an RCOG DPIA
- contain data protection clauses that meet the College's data protection standards outlined in this policy with differences and gaps risk assessed
- use the relevant College contractual template:
    - standard contract/service agreement template
    - IT software contract/service agreement template.
- where the contract proposed is different to the RCOG contractual templates, you and the IG Team are to complete a gap analysis and risk assessment as part of due diligence, and assess if the differences/gaps pose a risk to the College

Information Sharing

All sharing of personal data with external third party individual or organisation Data Controllers must be governed by a written Information Sharing Agreement. Please see the Records Management Policy and Procedures for details (section 2: Information Transfers).

International Transfers of Personal Data

All restricted transfers of personal data from the College to a controller or processor located outside of the UK must follow the Staff Guidance Notes and complete the following checklist:

1. **Is the College planning to make a restricted transfer of personal data outside of the UK?**
   You are making a restricted transfer if:
    a. the UK GDPR applies to your processing of the personal data you are transferring.
    b. You are agreeing to send personal data, or make it accessible, to a receiver which is located in a country outside the UK; and
    c. the receiver is legally distinct from you as it is a separate company, organisation or individual.

   If no, you can make the transfer. If yes go to Q2
2. **Do we need to make a restricted transfer of personal data in order to meet our purposes?**
   If no, you can make the transfer without any personal data. If yes go to Q3
3. **Are there UK 'adequacy regulations' in relation to the country or territory where the receiver is located or a sector which covers the receiver (which currently includes countries in the EEA and countries, territories or sectors covered by existing EU 'adequacy decisions')?**
   If yes, you can make the transfer. If no go to Q4
4. **Have we put in place one of the 'appropriate safeguards' referred to in the UK GDPR?**
   If yes, you can make the transfer. If no go to Q5
5. **Having undertaken a risk assessment, we are satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.**
   If yes, you can make the transfer. If no, go to Q6.
6. **Does an exception provided for in the UK GDPR apply?**
   If yes, you can make the transfer. If no, you cannot make the transfer in accordance with the UK GDPR.

Learning and Development

- All employees, Trainees, members, Officers, Board of Trustees/Committee members, volunteers, College representatives and suppliers:

    - Must complete induction, refresher and specific training, appropriate to their role, to help them understand how to process personal data in line with the Policy - e.g. complete the annual, mandatory data security awareness training and other training modules as and when required, such as Privacy and Consent (includes marketing consent), Data Protection Impact Assessments and Information Sharing.
    - Suppliers processing personal data on behalf of the College must meet our training standards and be assessed as part of contractual due diligence.
- All employees:
    - Processing special category personal data or with a dedicated IG role must attend the Advanced Data Protection training or equivalent and follow their departmental Special Category Personal Data Handling policy.

Governance

IGMG

The Information Governance Management Group (IGMG):

- Oversees the IG function of the College to ensure compliance is retained across the College
- Chaired by the SIRO
- Supported by the IG Team.

It is made-up of Directors from departments who process personal data and Subject Matter Experts (SME). The terms of reference are in Appendix B.

IG Leads

The IG Leads are employees nominated by the departmental Information Asset Owners (SLT member) to assist them with their IG responsibilities. Please see Appendix D for their terms of reference.

Performance Monitoring

- IG Dashboards – RCOG performance against key statutory compliance requirements are monitored at least quarterly, covering:
    - Individual Rights Requests – e.g. Data Subject Access Requests
    - Data Protection and Security Incidents – e.g. numbers logged as live, contained and closed with a severity rating and outstanding actions from lessons learned
    - Data Protection Impact Assessments – e.g. numbers logged with data protection risk rating
- Audit and Risk Committee – quarterly compliance reports highlighting progress against regulatory (Data Security and Protection Toolkit) and statutory requirements using the IG Dashboards (see above)
- Executive Committee – quarterly Data Security and Protection Toolkit (DSPT) project reports focusing on progress made against the DSPT for that year.

Roles and responsibilities

The data protection laws have clearly defined roles and responsibilities for all organisations. In the RCOG, we have defined and delegated as below.

A "**Data Controller**" (or Controller) is an individual or organisation who:

- decides to collect or process personal data
- decides what the purpose or outcome of processing is to be
- decides what personal data should be collected
- decides which individuals to collect personal data about

- obtains a commercial gain or other benefit from the processing, except for any payment for services from another controller
- processes personal data as a result of a contract between us and the data subject
- whose data subjects are the employees
- makes decisions about the individuals concerned as part of or as a result of the processing
- exercises professional judgement in the processing of the personal data
- has a direct relationship with the data subjects
- has complete autonomy as to how the personal data is processed
- has appointed processors to process the personal data on our behalf.

"Joint **Data Controllers**" are two or more individuals or organisations who:

- has a common objective with others regarding the processing
- processes the personal data for the same purpose as another controller
- use the same set of personal data (e.g. one database) for this processing as another controller
- designs the processing with another controller
- has common information management rules with another controller.

A "**Data Processor**" (or Processor) is an individual or organisation who:

- follows instructions from someone else regarding the processing of personal data
- is given the personal data by a customer or similar third party, or told what data to collect
- does not decide whether to collect personal data from individuals
- does not decide what personal data should be collected from individuals
- does not decide the lawful basis for the use of that data
- does not decide what purpose or purposes the data will be used for
- does not decide whether to disclose the data, or to whom
- does not decide how long to retain the data
- make some decisions on how data is processed, but implements these decisions under a contract with someone else
- is not interested in the end-result of the processing.

The College is predominantly a "data controller" when processing personal data, e.g. when we procure a service from a supplier under contract and the supplier is the "data processor". Sometimes we are a "joint data controller", e.g. many of our clinical quality projects and reviews involve sharing the "data controller" responsibilities with our NHS partners.

A "**Data Subject**" is a living individual who can be identified from the personal data or from additional information held, or obtained, by the RCOG.

The Policy defines the College's data protection roles and responsibilities:

- **Employees** – e.g. all employees of the RCOG (permanent, temporary and voluntary), contractors and consultants who have access to personal data - must
    - understand, keep up-to-date with, and comply with the Policy
    - complete their mandatory Data Security Awareness training every year, and within four weeks of joining the College – completion of the training is monitored and reported to Executive Director and Directors
- **Line managers'** must
    - apply the Policy across their team(s)
    - cascade data protection awareness communications to their team(s)
    - make sure their employees comply with the Policy

    - make sure their employees complete the mandatory Data Security Awareness training within given timescales
    - monitor suppliers and partners' compliance with the Policy through routine procurement and contract management activities, e.g. use appropriate contractual clauses and supporting information sharing agreements.
- **Information Asset Ownership** across the College has been delegated to Directors and some Information Governance Leads who must
    - understand what information assets their team(s) process(es)
    - understand its value to the College and the related approach, appetite and capacity for risks and opportunities in conjunction with the College's risk management standards
    - make sure information is managed according to the Policy.

  This includes making decisions about how information is processed e.g. what is collected, how it is used, who it is shared with, when it is deleted, and whether information risks are mitigated further or accepted by us.
- **Information Governance** (IG) **Leads** are employees who have been nominated by the Information Asset Owners and must
    - champion IG, including data protection, within their departments
    - be the first point of contact on all IG related matters, including data protection, within their departments
    - raise and monitor awareness of good IG practice within their departments, especially the processing of personal data
    - facilitate an annual assessment across their departments for the Data Security and Protection Toolkit.
- The **Information Governance Management Group** is responsible for overseeing all aspects of Information Governance (IG) at the College, including data protection. They must
    - ensure College compliance with statutory and regulatory requirements, e.g. GDPR and DPA
    - report to the Audit and Risk Committee.
- The **Senior Information Risk Officer (SIRO)** is responsible for implementing and leading on IG risk assessment and management processes with the College and must
    - Advise the Executive Team and Chief Executive Officer on the effectiveness of information risk management
    - lead on the management of security incidents and data protection breaches
    - Chair the IGMG
    - The RCOG SIRO is the Executive Director of Membership and Global, Kristen Morgan.
- The **Deputy SIRO** is the Head of Information and Governance, responsible for the delivery of IG best practice and
    - reports to the SIRO
    - is the named contact for external authorities, e.g. the ICO and NHS Digital
    - leads on data protection matters:
        - To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in partnership with the Caldicott Guardian
        - To define our data protection policy and procedures, all related policies, procedures and processes, and ensure sufficient resources are provided to support the policy requirement
        - To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT

        - To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management and SIRO to fulfil this work.
    - The Deputy SIRO is the Head of Information and Governance, Ciara Shimidzu.
- The **Caldicott Guardian** is primarily responsible for the protection of confidential, personal information and ensure it is used in line with the Caldicott Principles. The RCOG Caldicott Guardian is the Director of Clinical Quality, Daniel Wolstenholme.
- The **Information Governance (IG) Team** is part of the Research and Information Services department and must
    - provide day to day management of IG and data protection compliance across the College
    - provide advice and support to the IG Leads, Information Asset Owners and the wider organisation
    - assist the College with DPIAs
    - act as Administrator for the Toolkit
    - implement records management best practice
    - investigate security incidents and breaches
    - coordinate Individual Rights requests, e.g. Subject Access Requests (SARs).
- **Officers, Board of Trustees Members, Committee Members, Volunteers and all individuals given access to the College network/systems** to comply with the Policy when handling personal data on behalf of the College.
- **Trainees, members, College representatives and suppliers/contractors** must follow all the data protection requirements in their respective role descriptions, contracts, terms and conditions and/or Code of Conduct.

Policy Waiver

The College has a risk based approach to govern those situations that require the processing of personal data to deviate from this policy. In summary:

- The situation needs to be fully described
- The risks and mitigations captured
- The agreed waiver reviewed and signed off by the Information Asset Owner and Executive Director.

The Policy Waiver form in Appendix F must be completed and approved by senior management.

Data Protection Regulator: the ICO

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. Find out more about their organisation and structure on their website: https://ico.org.uk/about-the-ico/

RCOG ICO Registration

Reference number: Z6382904
Tier: Tier 1
Start date: 30 January 2002
End date: 29 January 2024.

For further advice concerning any aspect of this policy, please contact the Information Governance (IG) Team by email or call +44 20 7772 6309.

Appendices:

Appendix A: Glossary of Data Protection Terms

The **Data Protection Act 2018** is an Act of Parliament that enacted EU GDPR 2016, the new UK GDPR post-Brexit and established UK only derogations.

Data quality is a recognition that the accuracy, coverage, timeliness and completeness of data can significantly affect the value of its use.

A **Data subject** is a living individual who can be identified from the personal data or from additional information held, or obtained, by the RCOG. For example, a CCTV image which can identify someone when linked to building access control codes.

The **Freedom of Information Act 2000** provides the public with a general right of access to all information held by, or on behalf of, public authorities. Any individual or organisation may request any information held by a public authority. The public authority must tell the applicant (normally within 20 working days) whether it holds the information. If it does, it must supply it, unless an exemption applies. The RCOG, as an independent charity, is not a public authority, and is not directly subject to the Act. However, the College may hold information 'on behalf of' a public authority since it performs work for them under contract. Information relating to these activities may be caught by the Act.

The **UK General Data Protection Regulation (UK GDPR):** sets out data protection and privacy rights of all individuals within the UK since exiting the European Union. It also applies to transfer (export) of personal data outside the UK. UK GDPR came into force on 01 January 2021.

The I**nformation Commissioner or ICO** is responsible for the regulation of the Information Rights legislation across the UK, such as UK GDPR and DPA 2018. The Information Commissioner is appointed by the Queen and is independent of the UK Government.

Information Governance:

- encompasses the multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an organisation level,
- supports its immediate and future regulatory, legal, risk, environmental and operational requirements
- determines the balance point between two potentially divergent organisational goals: extracting value from information and reducing the potential risk of information
- defines the roles and responsibilities of all stakeholders involved in handling and managing College information.

Information governance compliance: ensures compliance with all statutory requirements governing the management of information, including rights of access under Freedom of Information and Data Protection legislation.

Information security ensures that RCOG information is not compromised by unauthorised access, modification, disclosure or loss.

Information sharing ensures that RCOG information is shared in a compliant, controlled and transparent manner.

Processing relates to all actions or handling of personal data by manual or automated means, e.g. data collection, erasure and destruction plus everything in between including recording, use, disclosure, sharing and storage.

Much of the information we process includes personal data about, e.g.:

- trainees and members of the College
- examination candidates
- visitors to the College
- users of College services, e.g. the website and library
- employees and officers working for the College
- contractors and suppliers of the College
- partners with the College, e.g. specialist societies.

Records management: processes and practices that ensure RCOG records are systematically controlled and maintained, covering the creation, storage, management, access, and disposal of records, in compliance with best practice, legal obligations and policy requirements.

A **Subject Access Request** is the right given, by Data Protection legislation, to an individual to ask for a copy of personal data processed by the College. The information must be supplied in an intelligible and permanent form unless this involves a disproportionate effort or the individual agrees otherwise. The RCOG may have to consider the Disability Discrimination Act requirements when providing personal data to an individual who may require the information to be provided in a certain format to consider a special need. Individuals have a right to correct inaccuracies in that information too – please see the RCOG Individual Rights Requests guidance for details.

Appendix B: IGMG Terms of Reference

- To provide strategic leadership for information governance and information risk management throughout the College, reporting into the Executive Committee, Officers (as appropriate) and Audit and Risk Committee with Director representation from key departments, namely those handling large volumes or high risk personal data, such as Clinical Quality, Membership, Education, Exams and People.
- To support, monitor and authorise the development of the Information Governance Framework and its implementation, including all accompanying policies, guidance and tools.
- To support the College's Information Governance network of IG Leads.
- To oversee the College's annual Data Security and Protection Toolkit Submission (formerly known as the IG Toolkit).
- To agree, support and monitor the annual Data Security and Protection Improvement plan to drive change, including plan revision and realignment to mitigate risk.
- To take ownership of information risk management, including monitoring compliance with the Information Governance Framework, reporting and escalating information risks as appropriate, taking corrective actions where necessary, and maintaining the IG Risk Register.
- To receive and consider reports into breaches of confidentiality and security and, where appropriate, undertake or recommend remedial action.
- To develop solutions and implementation programmes (including training and raising awareness) to ensure that the RCOG complies with developing information governance requirements.
- To ensure that each directorate fulfil their responsibilities and apply relevant information governance policies and controls.

- To support directors and managers with the implementation of information governance standards and policies, the management of information risks, and in promoting awareness throughout their areas.
- To support audit and assessment arrangements for information governance (internal and external).
- To ensure that the College's approach to information governance and information risk is effective in terms of resource, commitment and execution, and that it is communicated to all employees.
- To liaise with boards, committees and other working groups to ensure compliance with the College's Information Governance Framework.
- To provide a focal point for the resolution and/or discussion of information governance and risk issue.

Appendix C: IGMG Forward Plan

The remit of the IGMG is broad and requires detailed monitoring of information risk. As such, the following forward plan is in place to ensure there is sufficient time to complete this work and to assist with the IGMG meeting agenda.

The following "standing items" are included in the agenda for every meeting:

- Data Security and Protection (DSP) Submission and Improvement Plan – quarterly progress report
- IG Dashboards
- DSP Incident Register – review and escalation

The following "standing items" are only included in the agendas of these quarterly meetings:

- **January**
  - Review and sign-off the revised DSP policy and procedures framework
- **March**
  - Review and sign-off the revised DSP ways of working, employees training and communications framework
  - Review the Information Risk Register
- **June**
  - Review and sign-off updates to the Information Asset Register
  - Review and approve the proposed DSP Toolkit Submission for that year
- **October**
  - Review and approve the proposed DSP Toolkit Submission Plan for the next year.

Appendix D: IG Leads Terms of Reference

- To represent the IG needs of their department and be either a Head of Service or Team Lead role, supporting and deputising for the SLT Information Asset Owner
- To champion IG within their departments, including data protection and records management
- To be the first point of contact on all IG related matters, including data protection and records management, within their departments
- To develop a good knowledge and understanding of relevant IG, including familiarity with the policies and ways of working
- To complete all relevant IG training over and above the College's mandatory requirements, including Advanced Data Protection and relevant modules
- To raise and monitor awareness of good IG practice within their departments, especially the processing of personal data

- To attend IG Team organised meetings and events
- To actively engage with and contribute to the internal IG consultations, including the annual DSPT submission and DSP policy reviews to act as a contact point with the IG Team concerning the retention, disposal and transfer of records within the department
- To assess the records management procedures as they relate to each business function within their departments
- To assist employees and Officers on team records management procedures.

Appendix E: Policy Waiver Form

[Insert policy title here] POLICY WAIVER AUTHORISATION FORM - REF. [insert policy initials here]-000

Working together to handle personal data safely, respectfully and lawfully

Directorate:	**Information Asset Owner:**
Department:	**Information Asset Administrator/IG Lead:**
Proposed by departmental SLT member:	
Approved by Executive Director:	
Responsible member of staff name and job title:	**Email:** **Tel:**
Date of request:	
Information types – please list all the types and categories of information to be handled, e.g. paper copy examination forms**:** • …	
Description of information handling – please summarise the processes required that deviate from the cited policy, e.g. taking College information home or using personal webmail accounts**:** • …	
Duration of information handling: **START DATE:** **END or REVIEW DATE:**	
Insert here the policy controls that you require exempting from: • …	

What alternative measures have been considered? Please also explain why they have been rejected.
Does the information contain personal data? Y/N – please delete as appropriate. **If yes, what?** • …
Does the information contain any high risk, special category (aka sensitive) personal data or monitoring activities? Y/N – please delete as appropriate. **If yes, what?** …
List the information risks of the above handling – e.g. accidental loss of information, and unlawful access by 3rd parties at home. • …
List your proposed mitigations of the above risks: • …
INTERNAL USE ONLY BY IG TEAM OR IM&T
Severity: LOW/MEDIUM/HIGH
Mitigations accepted by IG Team/IM&T: Y/N – please delete as appropriate.
Further measures recommended: **1. …** **2. …** **3. …**
Authorisation **SIRO:**
Waiver logged in Information Risk Register: Y/N – please delete as appropriate.

Does the President / CEO need to be informed(Y/N):	**External/internal communication required:** **Y/N –** please delete as appropriate. **Details if applicable:**
Date waiver reviewed or closed :	