DATA PROTECTION POLICY (website version)

Data Protection Policy- IGPOL/03

Information Governance

Digital Division

April 2026

Review Frequency: Annually

Next review date: April 2027

Policy Owner: Data Protection Officer

Approval: Audit Finance and Risk Committee

Name	Date	Version	Comments
Data Protection Committee (for comment)	12/11/2025	3.11	Approved
SLT (for comment)	4/12/2025	3.11	Approved
Audit, Finance and Risk Committee	10/04/2026 (meeting on 02/04/2026)	3.12	Approved

Relevant Policies, Templates & Forms

The following policies, procedures, and guidance should be used or referred to when necessary alongside this policy. All policies and templates will be made available on the intranet once finalised and approved.

Reference	Document Name	Status
IGPOL/01	Information Governance Policy	Final- Published
IGPOL/02	Information Security Policy	Final-Published
IGPOL/03	Data Protection Policy	Final- Published
IGPOL/05	Records Management Policy	Final- Published
IGPOL/06	Corporate Retention Schedule	Final- Published
IGPOL/10	Archive and Collection Policy	Final- Published
IGPOL/12	Direct Marketing Policy	Final- Published
AUP	Acceptable Use Policy	Final- Published
IGPRO/01	Security Breach Procedure	Final- Published
IGPRO/02	Subject Access Request Procedure	Final- Published
IGPRO/03	Procedure for Handling Third Party Requests to Access Data on ePortfolio	Final- Published
IGPRO/05	Privacy Impact Assessments	Final- Published
IGNOTE /04	SAR Guidance- staff and volunteers	Final- Published
IGNOTE /05	Naming Convention Guidance	Final- Published
IGNOTE /06	Version Control Guidance	Final- Published
IGNOTE /07	Email Management Guidance	Final- Published
IGNOTE /08	Guidance for entering information onto ePortfolio	Final- Published
IGNOTE /09	Guidance for Clinical Audits on completing Rights Requests	Final- Published
IGNOTE /10	Good Handling Practice: Remote Working	Final- Published

IGNOTE /11	Email Scams and Phishing	Final - Published
IGNOTE /12	Crib sheet for all staff for personal data breaches	Final - Published
IGNOTE /13	Crib sheet for the BoT and the Emergency Response Group for personal data breaches	Final - Published
IGNOTE /14	Crib Sheet for communicating with suppliers during security breaches	Final - Published
IGNOTE /15	BCP for Security Breaches	Final - Published
IGNOTE /16	Checklist for managing consent	Final - Published
IGNOTE /17	WhatsApp Guidance- non-staff	Final - Published
IGNOTE /18	WhatsApp Guidance- Staff	Final - Published
IGNOTE /19	Children's Code Guidance	Final - Published
IGNOTE /20	Redaction Guidance	Final - Published
IGNOTE /21	Direct Marketing Guidance	Final - Published
IGNOTE /22	Committee Guidance on Information Security	Final - Published
IGNOTE /23	Co-Pilot Guidance	Final-Published
IGNOTE /24	Teams Meetings- Recordings, Transcripts, AI notes and Chat	Final- Published
IGNOTE /25	Guidance on Inactive SharePoint and Team sites	Final- Published
IGNOTE /26	Guidance on completing the ROPA	Final- Published
IGNOTE /27	International Transfer Crib Sheet	Final- Published
IGNOTE /28	Guidance on M365 Folder Structure	Final- Published
IGNOTE /29	Online meeting and communication tool guidance	Final- Published

IGNOTE /30	Transferring Born Digital Records to Archives	Final- Published
IGNOTE/31	Off-site storage guidance	Final- Published

Contents

1. Introduction

1.1. This policy establishes the College's commitment to adhering to UK Data Protection legislation, which is the UK General Data Protection Regulation (UKGDPR) in conjunction with the UK Data Protection Act 2018 and as amended by the UK Data Use and Access Act 2025. The College will therefore follow procedures that aim to ensure that all employees including temporary staff, workplace volunteers, interns, elected members or Officers, contractors, agents, consultants, partners or other servants of the College who have access to any personal data held by or on behalf of the College, are fully aware of and abide by their duties and responsibilities under the legislation.

2. Purpose of the Policy

2.1. In order to conduct its normal business, the RCPCH collects and uses certain types of personal information about living individuals. These include current, past and prospective members, trainees, staff, workplace volunteers, suppliers, research subjects and others with whom it has business, or with whom it communicates.

2.2. 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, partners, and the wider public in the College and its operations.

2.3. The College is fully committed to ensuring that it treats personal information lawfully and correctly and recognises that there are safeguards to ensure this in the UKGDPR.

2.4. This policy will describe legal standards for the use of personal information and guidance on individual's rights under the UKGDPR.

2.5. This policy will further detail the responsibilities of all members of staff, officers, trustees, volunteers, suppliers and college representatives to ensure corporate adherence to our responsibilities.

2.6. This policy relates to information held by the RCPCH and any organisation providing services on behalf of the RCPCH (i.e. data processors).

2.7. The RCPCH Data Protection Policy will be reviewed annually.. This will be reviewed each year by the Data Protection Committee, and it may be increased to every two years if deemed adequate.

2.8. Any member of staff breaching the RCPCH's Data Protection Policy will be subject to the established disciplinary procedure. In cases of deliberate negligence, where information is disclosed through purposeful criminal intent, individuals may be subject to criminal sanctions. Any action taken will be in accordance with the College's Conduct and Discipline Policy.

2.9. This policy should be read in conjunction with relevant Information Governance policies and other documents as detailed on pages 5 to 7.

2.10. This Policy will also apply to RCPCH staff in the devolved nations.

3. About UK Data Protection Legislation

3.1. The UK General Data Protection Regulation (UKGDPR), and the Data Protection Act 2018 as amended by the Data Use and Access Act 2025, are about the rights and freedoms of living individuals and in particular their right to privacy in respect of personal information.

3.2. UK data protection legislation stipulates that those who record and use personal information must be open about how the information is used and must follow good information handling practices. It applies to the collection, use, disclosure, retention and destruction of data.

3.3. Compliance with UK data protection legislation is monitored by the Information Commissioner Office (ICO) which is an independent regulatory body sponsored by the Department for Science, Innovation and Technology. The ICO is the supervisory authority for the purpose of RCPCH's processing activities.

3.4. The Regulation is applicable to any data controller or data processor that processes data in the UK. The Regulation also applies if a data controller is not in the UK but processes any personal data of UK residents or monitors behaviour of an individual within the UK.

3.5. Even where we use a data processor not based in the UK, as the data controller we still have certain responsibilities with regards to the data processor. For example, ensuring legally compliant contract clauses are in place, and that the processor has adequate safeguards in place to protect the privacy rights of individuals.

3.6. UKGDPR does not apply to certain activities for example processing carried out by individuals purely for personal/household activities.

3.7. UKGDPR applies to the whole of the UK, including the Devolved Nations.

4. Definitions

4.1. ***Personal data*** is any information relating to an identified or identifiable natural living person so someone who can be directly or indirectly identified from the information. This specifically includes name, location data, or online identifiers such as IP addresses and identification number or to one or more factors specific to the economic, cultural or social identifier of that person.

4.2. ***Special Category*** *data* means personal data consisting of information as to

- the racial or ethnic origin of the data subject
- their political opinions,

- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- genetic data
- biometric data
- their physical or mental health or condition,
- their sexual life

4.3. *Criminal offences data* means data relating to criminal convictions and offences, or related security measures. This includes information about criminal allegations, proceedings or convictions.

4.4. A *Data Controller* is the organisation that determines the purpose and the manner in which personal data may be processed. They make the decisions in regard to the data. The Data Controller in most cases will be the College.

4.5. A *Data processor* is an organisation or individual who are contracted to process data on our behalf. Although they may make their own day to day operational decisions, they should only process personal data in line with the data controller's instructions, unless required by law. They can be a company, legal entity or individual such as a consultant. Employees are not processors if they are acting within the scope of their duties as an employee.

4.6. Personal Data Processing is anything that you do with the personal data. This includes collecting it, receiving it, using it, disclosing it, storing it and destroying it. So even if the personal data is being held in our file store, we are processing it and therefore data protection legislation applies.

4.7. A *Data subject* is an identifiable individual who can be identified as the subject of the personal data.

4.8. A *third party* is an individual or organisation who is not the data subject, data controller or data processor.

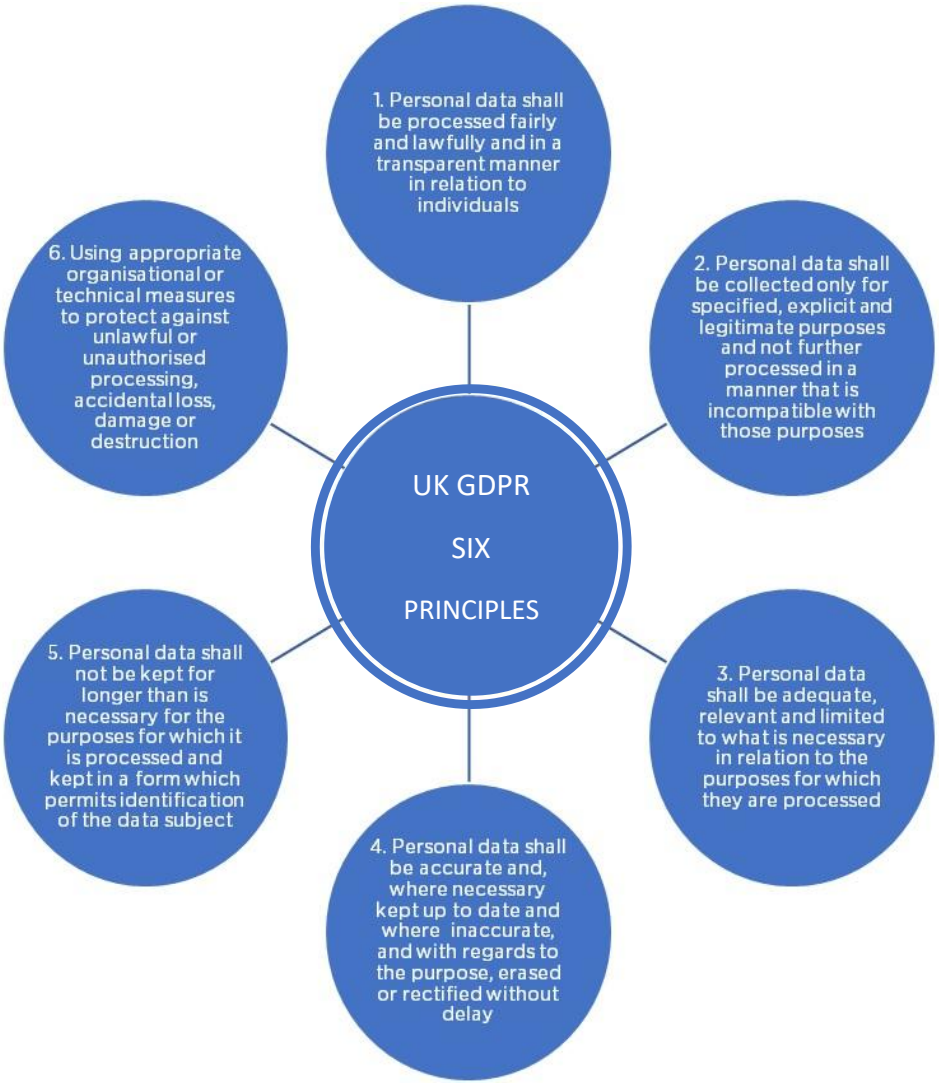
4.9. A *recipient* is the entity to which the personal data are disclosed.

4.10. *Information Society Service* is any service normally provided for remuneration, at a distance (remotely), by electronic means (online) and at the individual request of a recipient of services. This includes services where remuneration is not directly from the end user, e.g. a page is funded by advertising. It also covers not for profit services where those services can be considered as 'economic activity' in the more general sense. For example, apps, programmes, websites including search engines, social media, content streaming (e.g. video), news and educational sites.

4.11. Where this Policy references legislative articles and recitals, this will refer to the UKGDPR articles and recitals. However, this Policy covers both the Data Protection Act 2018 and UKGDPR as amended by the Data Use and Access Act (2025). Where this Policy references *'UK Data Protection legislation'* this will incorporate UKGDPR, Data Protection Act 2018 and amendments made by the Data Use and Access Act.

5. The Data Protection Principles

5.1. The UK GDPR (General Data Protection Regulation) sets out principles for handling personal data:



5.2. The College fully endorses and adheres to the Principles of Data Protection, as enumerated in UK Data Protection legislation.

5.3. The College will fully observe conditions regarding the fair collection and use of personal information.

5.4. The College will ensure that the minimum amount of personal information is collected as required to fulfil operational needs.

5.5. The College will only process data where there is a specific and legitimate purpose. If the data is transferred to the College Archive or is processed for scientific or historical research purposes or statistical purposes, this is considered a compatible purpose.

5.6. The College will take reasonable steps to ensure that all personal data is accurate and kept up to date and where data is found to be inaccurate will erase or rectify the data without delay, taking into account the reason for which it is processed.

5.7. The College shall store external stakeholder contact details on the College designated CRM (college's contact management system- customer relationship management) including all member and non-member details to avoid separate databases or lists by departments. This will support compliance with Principles 4 and 6. On rare occasions there may be an exception to this, but where this occurs alternative processes will be put in place by the team managing the contact details to ensure that the main CRM is kept up to date and vice versa.

5.8. The College will maintain the corporate retention schedule across all its Information Assets to ensure that personal data processed for any purpose or purposes shall only be kept for as long as business processes require or to fulfil legal obligations to Record Keeping, depending on which is the longest. RCPCH may also retain some data longer for public interest, or for medical or historic research purposes or statistical purposes. This data will be kept in compliance with the UKGDPR, in particular ensuring that appropriate organisational and technical measures are in place.

5.9. The College will establish processes within this policy to ensure that personal data will be processed in accordance with the rights of the data subjects.

5.10. The College will maintain and continue to develop an Information Governance programme to ensure that all data is managed securely, and that the appropriate technical and collegial measures are taken to safeguard personal information.

6. Lawful Purposes

6.1. Personal Data

6.1.1. All processing of personal data must have a lawful basis from one of the following:

- The individual has given consent (this can be implied consent for personal data only) or;
- The processing is necessary for the performance of a contract with the individual or to take steps to enter into a contract or;
- The processing is required under legal obligation or;

- The processing is necessary to protect the vital interests of the data subject or another person or;
- The processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject or;
- The processing is necessary for recognised legitimate interests as detailed in the Data Use and Access Act.
- The processing is in the functions of public interest or in the exercise of official authority vested in the controller.

6.2. Special Category Data

6.2.1. Special Category data will only be processed where it meets one of the criteria above and:

- The College has obtained the *explicit* (see section 8 on consent) consent of the data subject or;
- It is required by law to process the data for employment, social security or social protection law purposes, or a collective agreement or;
- It is necessary to process the information in order to protect the vital interests of the data subject or another, and consent cannot be given or reasonably sought because the data subject is physically or legally incapable of giving consent or;
- The information is required for scientific, including medical, or historical research or statistical purposes. If for medical research the College has approval from the Health Research Authority to conduct these activities or explicit consent from the data subjects. or;
- The information has been manifestly made public by the individual or;
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity. or;
- Processing is necessary for reasons of substantial public interest which is proportionate to the aim pursued and which contains appropriate safeguards or;
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

6.2.2. The college must also put in place an appropriate policy document for all of the substantial public interest conditions as well as for the employment, social security and social protection condition in order to

retain compliance with the UK Data Protection Act 2018. This includes having:

- A Schedule 1 of the Data Protection Act 2018 condition
- Procedures for compliance with the data protection principles
- Retention and erasure protocols in place

6.2.3. These are to be documented using the College's Appropriate Policy Document template (Appendix A). These are retained by the Information Governance Team and are available on request.

6.2.4. The main processing activities that this applies to are:

- Staff data
- Membership data
- Equality and Diversity data
- Covid Data
- International Volunteer data

6.3. Criminal Offence Data

6.3.1. There are also specific obligations for the processing of data relating to criminal offences and convictions. The legal grounds for processing this type of data are detailed in the Data Protection Act 2018. We cannot retain comprehensive registers of these, and we can only process this data where we are legally obliged to do so. For example, if we need to carry out DBS checks where members of staff, volunteers or trustees are working with children and young people or vulnerable adults unsupervised on a regular basis. The Framework for Managing People Policy on Recruitment of Ex-Offenders outlines the College's Policy in relation to requesting, using and retaining DBS checks in line with the Rehabilitation of Offenders Act 1974.

6.3.2. The College will record and maintain records of the processing activities that process criminal offences ROPA (Record of Processing Activities). This is managed centrally by the Information Governance team and retains a record of all of the college's personal data processing activities.

6.3.3. Where we require DBS checks to be undertaken, we will not retain full copies of DBS checks, only a log recording that the check has been undertaken, the date, the unique reference number and the outcome.

6.3.4. Where the processing relies on a Schedule 1 condition, an appropriate policy document (appendix A) will need to be completed. These will be retained and reviewed annually by the Information Governance team and are available on request.

6.4. Personal data relating to Children & Young People

6.4.1. UKGDPR states that children merit specific protection with regard to their personal data because they may be less aware of the risks involved.

6.4.2. If processing data through online information society services, for example an online forum, online form or social media where there is some kind of remuneration (this does not have to be monetary), then parental consent is required for any child aged 12 and under. For the full definition of an Information Society Service, see section 4.9 of this Policy. We will have appropriate verification measures in place to verify age, taking into account what type of data we are asking for and the risk to the individual.

6.4.3. Where online services are likely to be used by children DUAA states a specific obligation to take into account CYP needs, including considering:

6.4.3.1. How children can be best protected and supported;
6.4.3.2. The fact that children are less aware of the risks and consequences involved and therefore merit specific protection; and
6.4.3.3. The different needs children have at different ages and developmental stages.

6.5. We will comply with the ICO's statutory Age Appropriate Design: Code of Practice when developing any information society services that are likely to be accessed by children in the UK. For example, apps, programmes, search engines, social media platforms, streaming services, news and educational websites. It is not restricted to services specifically directed at children.

6.6. Any processing of personal data of a child or young person that is not on an information online service, shall only take place to the extent that such consent is given or authorised by the holder of parental/guardian responsibility over the child or young person. If the child or young person is under 18, generally the college will ask for parental/ guardian and child/young person consent, except in certain circumstances where this is not appropriate.

6.7. Where privacy notices are aimed at children and young people, the College will aim to write these in clear and simple language which is understandable to target age group.

6.8. If we are collecting personal data relating to children and young people for the first time, or using the data for a new purpose, we will carry out a Privacy Impact Assessment.

6.9. We will not use a child's/young person's data to make solely automated decisions which will have an impact on them, such as using a child's personal data to automatically (without any human intervention) profile them to make healthcare decisions that will impact them. The college will not undertake any behavioural advertising or profiling for marketing purposes in relation to children or young people.

7. Transfer of personal data outside of the UK

7.1. The College will adhere to Chapter 5 of the UKGDPR in regard to the transfer of personal data outside of the UK.

7.2. A restricted transfer occurs where personal data is being made accessible to a receiver where UKGDPR does not apply and the receiver is a separate organisation or individual (i.e. they are not someone employed by the College). For example, if uploading personal data onto a website which it is anticipated will be accessible outside of the UK, this would be a restricted transfer.

7.3. The College will ensure that all its information assets are not transferred to a country or territory outside the UK unless there are suitable safeguards, and in so doing complies fully with the specific terms of the UKGDPR relating to this, namely:

- That the country or territory can ensure that an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data as the UK Government has made an adequacy regulation. The list of countries with an adequacy regulation are available on the ICO website.
- That there is an International Data Transfer Agreement or an International Data Transfer Addendum with EU Standard Contractual Clauses in place;
- The college has entered into a bespoke contract governing a specific restricted transfer with the receiver which has been approved by the ICO.
- There is an exception, either the data subject has given explicit consent to the transfer or the transfer is a one-off and;
    - The transfer is necessary to perform or fulfil a contract that the data subject has entered into or is planning on entering into or where the contract benefits another individual whose data is being transferred.
    - There is a UK law which implies or states that the restricted transfer is allowed for important reasons of public interest.

- To establish a legal claim, to make a legal claim or defend a legal claim.
- To protect the vital interests of an individual where they are physically or legally incapable of giving consent.
- There is a compelling legitimate interest.

7.4. The college will conduct a transfer risk assessment for international transfers subject to appropriate safeguards in 7.3, where there is no adequacy decision.

7.5.

7.6. Any risks in relation to restricted transfers will be added to the Privacy Risk Register which is monitored by the Data Protection Committee.

7.7. Wherever possible, the College will use technological solutions that do not require the transfer of data outside the UK or a country with an adequacy decision such as the EU, for example they use servers within the UK to store the data.

7.8. Even if the College is legally allowed to transfer data outside of the UK, RCPCH must still ensure that appropriate organisational and technical security measures are in place to transfer the information.

8. EEA and Swiss Data Protection Representative

8.1. As the college processes personal and special category data relating to EU data subjects and Swiss data subjects, the college is required to employ an EEA Representative to comply with EUGDPR and a Swiss Data Protection Representative to comply with Switzerland Federal Act on Data Protection (FADP, Article 14) . The EEA and Swiss Representative will act as the point of contact for European Supervisory Authorities and EU data subjects, and Swiss Supervisory Authorities and Swiss data subjects and will be appointed in writing.

8.2. The contact details for the college's EEA and Swiss Representative will be published on the college's privacy notices, where applicable.

9. Accountability and Governance

9.1. Under Article 5(2) the College, as data controller, is responsible for and must be able to demonstrate compliance with these principles. Therefore, the College will maintain records on its processing activities as evidence of its compliance by maintaining a ROPA (Record of Processing Activities) which will be made available to the ICO and our EEA and Swiss Representative as required.

9.2. In line with UKGDPR the College will adopt a privacy by design and default approach when setting up a new process or system that will involve the processing of personal data. This is so that data protection is embedded in

our processes. Only the minimal amount of personal data will be used for the purpose. Data will be anonymised or pseudonymised where possible, particularly when transferring data.

9.3. The College will follow its Privacy Impact Assessment Policy. The College will always undertake a Privacy Impact Assessment where processing will potentially lead to high risks to individuals.

10. Consent

10.1. Where the College is relying on consent for the processing of personal data, the College will ensure that all consent, regardless of whether it is implicit or explicit, will be:

- Fully informed;
- Freely given;
- Specific to the purpose and channel of communication;
- Show an indication of an individual's wishes.

10.2. Consent does not last forever; it must be refreshed. When deciding how long consent is valid for, it is important to consider the context in which consent was gained and what would be a reasonable expectation of the individual.

10.3. An individual has the right to withdraw consent at any time. In exceptional circumstances, we may continue to process the data under alternative beother legal grounds but only when there are strong grounds to do so, taking into consideration the individuals right to withdraw consent.

10.4. Implicit consent is where consent is assumed from the involvement in a transaction (for example, purchasing a publication online, or registering for an examination).

10.5. Implicit consent must still be able to demonstrate that you have gained consent, but it does not have to be confirmed in words, it can be inferred by a person's positive actions where it is obvious. For example, you ask someone to complete a survey about how they found the delivery of one of our exams. By submitting the survey, they are clearly indicating their consent for the purposes of the survey. However, they are not consenting for any further uses of the information.

10.6. For the consent to be explicit the data subject must confirm consent in words such as a signature, a tick box or an email.

10.7. Where consent is relied on for Direct Marketing, in line with the college's Direct Marketing Policy, a clear opt in will be provided.

10.8. All consent must be recorded and be retrievable and retained for as long as the data that is being processed is retained. Where possible, staff will use the college's consent form template. Consent forms should be saved in the College's consent form database with restricted folders for CYP consent forms. It is important that, if required, consent forms can be matched to the activity for which consent was gained. For example, if consent is given to use a photo for a publication, a photo should be attached to the consent form so that the individual's consent can be identified.

11. Individual Rights

11.1. The GDPR gives individuals certain rights regarding their personal data. RCPCH will only answer rights requests where it is the data controller. These are:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object
- Rights in relation to automated decision making and profiling.

11.2. Requests can be made verbally or in writing.

11.3. Requests will be free of charge, unless considered excessive or manifestly unfounded.

11.4. The college commits to the processing of all personal data in compliance with these rights (unless a data protection law exemption applies). Further details on how the College will comply are in Appendix B.

11.5. Where RCPCH is not the data controller, they shall forward the request onto the data controller but will inform the requester that they have done so, unless there is a contractual agreement which states otherwise.

12. Data Protection Complaints

12.1 Data Subjects will be informed via privacy notices of their right to complain about the way their personal data has been handled. The college will acknowledge all data protection complaints within 30 days and will respond without undue delay.

12.2 The College will set out its complaints process in the Data Protection Complaints Procedure and provide a complaints form.

13. Disclosure of Information to outside agencies

13.1. There are some exemptions to disclosing personal data to third parties, namely:

- Safeguarding National Security
- The prevention or detection of crime
- Regulatory activity
- Information required by law or by a court order

13.2. Any requests from third parties for the disclosure of personal or Special Category data must be passed to the Information Governance team who will respond on behalf of the Data Controller.

13.3. Each request will be judged on a case by case basis by the Information Governance team and dealt with in line with the Procedure for Handling Third Party Requests.

13.4. Where disclosure is necessary for the recipient to perform their public tasks or functions, the responsibility will lie with the requesting organisation to ensure they can evidence this legal ground. The college may still undertake its own assessment and may choose not to disclose the information if they have objections.

14. Data Processors

14.1. Under UKGDPR, a data processor also has legal liability if there is a breach of the Regulation as a data subject can bring action against them and the ICO can also fine them. It is important that any third parties that are processing data on our behalf are aware of their liabilities.

14.2. As a data controller, the College must have a binding contract in place with any third party that processes data on the College's behalf and this will cover the clauses outlined in Article 28 and 29 of the UKGDPR. The college will maintain template contract clauses on the college's contract database.

15. Roles and Responsibilities

15.1. Chief Executive

- The *Chief Executive* as the Chief Officer retains overall responsibility for compliance with the regulation but will delegate responsibilities throughout the College.
- The Chief Executive is part of the Emergency Response Group for personal data breaches.

15.2. Trustees

- Trustees will be informed of any personal data breaches that have been reported to the ICO, or of any data protection complaints.
- SLT may also decide to inform the Trustees of other high privacy risks, as appropriate.

15.3. Audit, Finance and Risk Committee

- The AFRC is responsible for approving this Policy.

15.4. SLT

- SLT are responsible for reviewing and approving Information Governance Policies and Procedures, once these have been approved by the Data Protection committee.
- SLT will be notified of any significant personal data breaches.

15.5. Data Protection Committee

- The Data Protection Committee has representation from each division.
- The Data Protection Committee is responsible for reviewing and approving all Information Governance Policies and Procedures.
- The Data Protection Committee is responsible for maintaining the Privacy Risk Register and escalating any significant risks to SLT.
- The Data Protection Committee oversees Information Governance at the College. Effective information governance ensures compliance with relevant information governance legislation such as data protection legislation, but also leads to better business efficiency and cost savings through effective records management.

15.6. Senior Information Risk Owner (SIRO)

- The SIRO is responsible for owning any medium to high risk that cannot be appropriately mitigated by a PIA.
- The SIRO will chair the Data Protection Committee in the absence of the Head of Information Governance.

- The SIRO is informed of personal data breaches that reach a certain level, as defined in the RCPCH Security Breach Procedure and is responsible for approving any costs associated with the breach. The SIRO is also part of the College's Emergency Response Group.

15.7. Head of Information Governance

The Head of Information Governance also holds the role of Data Protection Officer. A *Data Protection Officer* is a legal requirement for RCPCH. On behalf of the Data Controller, the College Head of Information Governance has the day to day responsibility for ensuring that the College complies with the UKGDPR, informing and advising RCPCH on data protection issues and monitoring compliance, and will:

- Provide advice on compliance with the UKGDPR;
- Create and ensure the dissemination of Information Governance policies and procedures;
- Ensure that all processing activities involving personal data by the RCPCH are recorded on the Information Asset Database;
- Regularly review and audit the way personal information is managed, and that methods of handling personal information are regularly assessed and evaluated;
- Be the first point of contact for the ICO;
- Lead on processing rights requests and third party disclosure Requests ensure that they are dealt with efficiently and effectively;
- Lead on the Security Breach Procedure;
- Ensure that Data Protection and Information Security training is made available to all staff in the College;
- Take legal advice on matters relating to the Regulation where necessary and in consultation with the Head of Governance;
- Own this Data Protection Policy and have responsibility for reviewing this Policy for adequacy and monitoring compliance with it.

15.8. Managers

Managers will ensure that their staff are sufficiently aware of this policy and the associated guidance, protocols and agreements to carry out their role. They will:

- Supervise appropriately everyone managing and handling personal information;
- Ensure that members of their team deal quickly and promptly with any right of access requests;
- Ensure that they have sufficient resource to carry out their Information Management responsibilities and that their staff are made available for information management training;

- Appoint lead officers within the directorate to assist the Information Governance team in coordinating rights requests;
- Ensure members of their team have undertaken mandatory Data Protection Training and refresher training after two years.

15.9. Divisional Executive Directors

- Divisional Executive Directors are responsible for ensuring that their division is compliant with the Data Protection Policy.
- If the College is fined by the ICO for non-compliance with UKGDPR, the Division which caused the breach will be responsible for paying the fine from their budget. Fines can be as high as £17.5 million or 4% of turnover.

15.10. Officers, Suppliers, Volunteers, Committee Members, Trustees and College Representatives

- All are required to comply with this Policy when handling personal data on behalf of the College.

15.11. All users

All users must adhere by the data protection principles, and in particular must:

- Ensure that all copies of personal data are securely processed including obtaining, recording, retrieval, consultation, holding, disclosing, use, transmission, erasure, destruction;
- Ensure that when Information is shared on a case by case basis consent has been obtained from the individual;
- Ensure that where bulk sharing with another organisation or a different service area of the RCPCH that advice has been sought from the Information Governance team and an Information Sharing Agreement is in place and that they follow the Information Sharing Policy;
- Ensure that all personal or special category information is secured from loss, corruption, damage, disclosure;
- Undertake mandated training to ensure understanding of their responsibilities;
- Ensure that they take appropriate measures when handling or transferring personal data and ensure that confidential information is not disclosed outside of the workplace;
- If asking a third party to undertake processing of personal data on behalf of the College, contact the Information Governance team to seek further advice on appropriate binding contract clauses to meet our UKGDPR requirements.
- Where personal or special category information is being collected for a new operational purpose, the employee must inform the Information Governance team;
- Ensure that all information collected is for a specific purpose only and is accurate and not excessive;
- Ensure that they pass all requests for disclosures for personal or special category information to the Information Governance team promptly;

- Process college personal data in an appropriate way and in line with college policies and do not use it in an unauthorised, malicious or inappropriate way which is against the purposes for which the personal data was obtained.
- If responsible for information assets, inform the Information Governance team so that this can be added to the information asset database. See the Information Governance Policy for more detail on Information Assets.
- Express opinions relating to individuals in a professional manner;
- When required, employees will assist the Information Governance team with compiling information requested as part of a Subject Access Request or disclosure under one of the exemptions outlined in the Regulation. All requests should be dealt with promptly and as a matter of priority.

16. Training

16.1. Data Protection and Information Security Training is mandatory for all new staff including temporary staff, and trainees. Refresher training must be taken by all staff every year. Data Protection training is monitored and reported on annually as part of the evidence requirement submitted to the NHS DSP toolkit.

17. Governance

17.1. All data protection issues should be escalated to the Information Governance team and put through Topdesk (internal enquiries system). The SIRO may also be informed of issues where appropriate, particularly where the criteria are met in the security breach procedure. The Head of Information Governance will decide whether the Data Protection Committee needs to be informed. The Committee may also then decide to escalate any issues to SLT and then possibly the Audit, Finance and Risk Committee and the Board of Trustees, if necessary.

17.2. The Data Protection Committee will meet regularly and will monitor and review Data Protection processes and practices and the privacy risk register.

Appendix A - Appropriate Policy Document: Special Category/Criminal Offence Data

The RCPCH complies with the requirements of the General Data Protection Regulation (2016/679 (EU UKGDPR) and the Data Protection Act 2018, as well as other associated legislation.

Article 9(1) of the UKGDPR defines special category data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

This Appropriate Policy Document (APD) explains how the RCPCH processes special category data of our members in line with the legislation under Schedule 1, Part 2, Paragraph 5(1).

Description of data processed

The RCPCH processes the following special category data of: We collect it for the following purposes: The data is collected through:

Schedule 1 condition for processing

We process special category data under the following UKGDPR Articles:

- **Article 6():**
- **Article 9()():**

As the data is processed for reason of XX we also rely on the following DPA 2018 Schedule 1 condition:

- **Schedule 1, Part X, Paragraph X**:

Further information can be found in the following privacy notices:

Procedures for ensuring compliance with the principles

Article 5 of the UKGDPR maintains data shall be:

- Processed lawfully, fairly and transparently
- Collected for specific purposes
- Adequate, relevant and limited to what is necessary
- Accurate and where necessary kept up to date
- Kept for no longer than necessary
- Stored securely to maintain integrity and confidentiality

The controller must comply with these principles and be able to demonstrate compliance.

When processing special category data, RCPCH complies with the principles in the following ways:

Accountability principle
We have put in place the following internal processes in order to achieve compliance with Article 5(2):

- The College has appointed a Data Protection Officer
- We keep a record of processing activities (ROPA) through our information asset register. All activities involving personal and special category data are listed on the register.
- We carry out DPIAs for any activity relating to any activity involving large amounts of personal or special category data, monitoring, surveillance or profiling activities, or a new system or software. We keep a register of all PIAs and our PIA policy is reviewed annually.
- Our policies are regularly reviewed and cover data protection and confidentiality, information governance, records management, information security, information sharing, DPIAs
- We maintain logs of security incidents, data subject rights requests and information sharing, along with appropriate procedures.
- All staff receive data protection training.

Principle (a): lawfulness, fairness and transparency

We ensure data is only processed when a lawful basis applies and that data subjects are informed of the legal basis and purposes of the processing. This information is provided in a privacy notice, including the XX privacy notice.

We rely on Articles 6() and 9()(), with Schedule 1()() to process special category data about our XX as it is....

Principle (b): purpose limitation

We process special category data to

Information about why we collect information and who we share it with is available in the relevant privacy notice.

Principle (c): data minimisation

The information we collect is proportionate to the purpose...

Principle (d): accuracy

As the data is stored in

Principle (e): storage limitation
Information is retained according to our retention schedules to the best of our ability (e.g. in terms of system capability). If we no longer have a legal basis for processing, we will delete the information unless it is retained for archiving purposes. All assets involving personal and special category data are listed in the information asset register.
Principle (f): integrity and confidentiality (security)
Policy and organisational measures College work is carried out in line with the Information Security Policy and Records Management Policy. Any hard copy information is processed in line with our Physical Security Policy. The Data Protection Committee meet regularly to ensure suitable information security and compliance throughout the College. All members of staff attend mandatory data protection training. The Data Protection Office and SIRO are appropriately trained. **Technical measures** All College electronic systems have appropriate access controls and are assessed to meet appropriate security, including PIAs and penetration testing. The RCPCH has also completed Cyber Essentials Plus and the NHS Data Security and Protection Toolkit. Where possible, role-based restricted access, anonymization/pseudonymisation, and encryption are used.

Retention and erasure policies

Special category data is held in XX.This information is held in line with our records retention schedule

APD review date

This policy will be retained for six months after the processing ends and will be reviewed annually.

Appendix B- Process for Handling Rights Requests

1. Processing Rights Requests

1.1. All rights requests will be forwarded to the Information Governance team as soon as they are received, who will respond on behalf of the Data Controller within one month, or within two months if the request is particularly complex.
1.2. The College may ask for further ID if required to verify the individual.
1.3. The College may refuse a request if it is manifestly unfounded or excessive, particularly if repetitive. In this instance, the College may request a reasonable fee to deal with the request or refuse to deal with the request. The Information Governance team will document any decisions.
1.4. If refusing a request, the College will inform the individual without undue delay and within one month of receipt of the request, the reasons for not taking action, their right to complain to the ICO and their ability to seek to enforce this right through a judicial remedy.
1.5. All requests will be recorded on the request log by the Information Governance team and appropriate documentation retained.

1.6. The Right of Subject Access

1.6.1. The Regulation allows individuals to find out what information is held about themselves by an organisation, regardless of format. This is known as the right of access.

1.6.2. All requests for personal information must be dealt with in accordance with the RCPCH Subject Access Request procedure.

1.7. The Right to be Informed

1.7.1. Under GDPR individuals have the right to be informed about how and why their personal data is being used.
1.7.2. Privacy notices will be provided at the point of collection of the personal data or, if not possible, as soon as possible after the data is collected (and within one month). The privacy notices will inform individuals about how and why their data is processed and will cover the requirements set out by Article 13 and 14 of GDPR.

1.7.3. Privacy notices will be made easily accessible, transparent, intelligible and concise and written and targeted to its audience.

1.7.4. The Information Governance team will advise staff on how to write privacy notices.

1.8. The Right of Rectification

1.8.1. Article 16 of GDPR provides the right for an individual to request that inaccurate information about them is rectified.

1.8.2. Each request will be judged on a case by case basis by the Information Governance team.

1.8.3. Whilst investigating the College will not process the data further other than to store the data, except in exceptional circumstances.

1.8.4. After investigation, if the information is found to be inaccurate, the College will amend the record and inform the individual of the outcome and document why and when the information was updated.

1.8.5. If the College believes the record is accurate, then the Information Governance team will respond to the individual informing them of why the college will not be amending the data, an explanation of the decision, and informing them or their right to make a complaint to the ICO and their ability to seek to enforce their rights through a judicial remedy. The College will also make a note on the system or document that the individual challenged the accuracy of the data and their reasons for doing so.

1.8.6. If information has been given to a third party, the College will inform the third party of any changes and will also inform the data subject that information has been shared with the third party.

1.9. Right to Restrict Processing

1.9.1. Under certain circumstances, an individual can request that a data controller restricts the processing of their personal data so that the data controller can only store it and not use it in anyway. This request is only valid if:

1.9.2. The individual has asked that inaccurate data is rectified (a right to restriction request).

1.9.3. There are no legal grounds to process the data and the individual does not want the College to destroy the data.

1.9.4. The College no longer needs the personal data but the individual needs to keep it to establish, exercise or defend a legal claim.

1.9.5. Or the individual has objected to the data being processed and the College is considering whether there are still legitimate grounds to process the data which over the legitimate interests of the individual.

1.9.6. If the data subject request to restrict processing is successful, the College will only store the information required in line with the data subject's wishes.

1.9.7. If the data is also held by third parties, we will inform the third party of the request.

1.10. The Right to object to processing

1.10.1. An individual can ask a Data Controller to stop processing their personal data where it is processed:

- based on legitimate interests or the performance of a task in the public interest/exercise of official authority;
- for direct marketing (including profiling); or
- for purposes of scientific/historical research and statistics.

1.10.2. Where there is an objection to direct marketing, the College will immediately stop processing the data for this purpose and update Care. This is an absolute right.

1.10.3. The College will ensure that the data subject will be given the option to opt in to any direct marketing processes except where these are based on performance of a contract or legitimate interests, where legally appropriate. This includes the passing of personal data to third parties.

1.10.4. The College will maintain a list on Care of mailing preferences.

1.10.5. All requests from data subjects to opt out will be recorded on the College CRM, Care.

1.10.6. Where the objection is not based on direct marketing, the Information Governance team will deal with these on a case by case basis.

1.10.7. If the objection is based on legitimate interests, the College will carefully consider whether its legitimate interests overrides the legitimate interests of the individual.

1.10.8. If the research is being carried out for public interest purposes, the College does not have to comply.

1.10.9. If services are offered online, the data subject will be given the option to object online.

1.10.10. Individuals will be informed about their right to object through the privacy notice given when collecting the data.

1.10.11. The College will not comply if the processing is necessary for the establishment, exercise or defence of legal claims.

1.10.12. If the College agrees to the objection and stops processing the data, they will also inform any third parties who hold the data.

1.10.13. Where processing NHS digital data, the national opt out will be applied where appropriate.

1.11. Right to be forgotten

1.11.1. Under GDPR a data subject has a right to be forgotten. This only applies where:

- The personal data is no longer necessary for the purpose for which it was processed;
- The College is relying on consent to process the data and the individual withdraws consent;
- If an individual objects to processing based on legitimate interests and there object is upheld by the College;
- Processing is for direct marketing purposes and the individual has objected.

- The College does not have legal grounds to process the data
- The College legally obliged to destroy the data; or
- The College have processed the data to offer information society services to a child.

1.11.2. The right to be forgotten is particularly strong with regards to a child's personal data. Therefore, where processing a child's data based on consent, particularly weight will be given to the request.

1.11.3. It is important to minimise the amount of personal data the College is holding and to anonymise where possible.

1.11.4. The College does not need to comply with the request where it is processing personal data for the following purposes:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

1.11.5. The College will not delete trainee records whilst a trainee is still training as this is required to fulfil our legal obligations with the GMC and also because it is in the public interest relating to public health.

1.11.6. If processing special category data, the right to erasure will not apply:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of confidentiality (eg a health professional).

1.11.7. Where the College has disclosed the information to a third party, they will inform the third party of any erasures.

1.12. The Right to Data Portability

1.12.1. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. A data subject can move, copy or transfer data easily from one IT environment to another.

1.12.2. This right is only available for personal data that either:

- An individual has provided to the RCPCH (or data controller);
- The data has been processed using the individuals consent or for the performance of a contract; and
- Processing is carried out by automated means (by machine and not paper records);

1.12.3. The information will be provided free of charge.

1.12.4. If the request is successful, the personal data will be provided in a structured, commonly used and machine-readable form, such as Word, Plain Text, CSV or Excel.

1.13. Rights in relation to automated decision-taking, including Profiling

1.13.1. Automated decision making is a decision made by automated means. This includes profiling (using automated means to evaluate certain things about an individual) and the potential use of AI to support decision making relating to an individual.]

1.13.2. Where the college is processing personal data for the purposes of automated decision making, and the decision will have a legal or similarly significant effect on the individual, the college will:

1.13.2.1. Provide individuals with detailed information about its use of automated decision making systems including the decision-making logic and data used;

1.13.2.2. Offer the right to request human review

1.13.2.3. Conduct a privacy impact assessment to evaluate the risk and benefits with a focus on privacy, fairness, bias and discrimination;

1.13.2.4. Implement accountability measures such as regular audits and compliance checks.

1.13.3.

1.13.3.1.

1.13.4. The college will only undertake automated decision using special category data where one of the following safeguards apply:

1.13.4.1. The college has explicit consent from the data subject; or

1.13.4.2. The processing is necessary for a substantial public interest.

1.13.5. The College will not carry out profiling, or automated decision making which has a legal or similar impact, on children except in exceptional cases and where legal to do so.

1.13.6. If the College undertakes any new profiling or automated decision making activities,

1.13.7. If the College undertakes profiling activities, it will only keep the minimum information necessary and have appropriate retention policies in place for the profile created.