The Royal College of Pathologists
Pathology: the science behind the cure

DATA PROTECTION POLICY **January 2022**

1. Introduction

1.1 This Policy sets out the obligations of the Royal College of Pathologists (referred to as "the College" for legal reasons) regarding data protection and the rights of current, past and prospective Fellows, and members, staff, suppliers, clients, customers, and others with whom it has business or with whom it communicates ("data subjects") in respect of their personal data under the Data Protection Act 2018 ("the Act") and the UK General Data Protection Act and Regulation ("the Regulation").

1.2 The College wholly owns RCPath Trading Limited as a subsidiary company. Data is shared between the College and the wholly owned subsidiary for the subsidiary's activities, which are RCPath Consulting and the commercial letting of conference and other space within College owned premises.

1.3 The Act and Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.4 This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the College, its employees, those termed as 'volunteers', agents, contractors, or other parties working on behalf of the College.

1.5 The College is committed to ensuring that it processes personal information lawfully and it places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1.6 Compliance with data protection legislation is the responsibility of all members of the College who process personal data.

2. Data Processing Principles

2.1 This Policy aims to ensure compliance with the requirements of the Act and Regulation by ensuring that personal data is only processed in accordance with the following data protection principles:

a. processed lawfully, fairly, and in a transparent manner in relation to the data subject.

b. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Act and Regulation in order to safeguard the rights and freedoms of the data subject.

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.2 As a data controller, the College must be able to demonstrate compliance with the six data processing principles detailed above. To this end, this Policy is to be reviewed regularly to determine if it's being deployed effectively throughout the College. The review will also consider whether adequate resources are available to ensure the ongoing effectiveness of this Policy.

3. Lawful, Fair, and Transparent Data Processing

3.1 The Act and Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Act and Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b. processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;

c. processing is necessary for compliance with a legal obligation to which the controller is subject;

d. processing is necessary to protect the vital interests of the data subject or of another natural person;

e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

3.2 Where a special category of personal data, as defined by Article 9 of the UK GDPR, is processed, this shall be for one of the defined 10 exceptions as defined in the Article 9:

a. Explicit consent.

b. Employment, social security and social protection law.

c. Vital interests.

d. Not-for-profit bodies.

e. Made public by the data subject.

f. Legal claims and judicial acts.

g. Substantial public interest conditions.

h. Health or social care.

i. Public health.

j. Archiving, research and statistics

3.3 The College is mandated to have an appropriate policy document (APD) in place when processing special category (SC) personal data or criminal offence (CO) data in reliance on a condition in Part 1, 2 or 3 of Schedule 1, DPA 2018.

3.4 The full list of Conditions on which the College rely to process SC and CO data can be found at Appendix 1 to the College's APD.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 To conduct its normal business, the College collects and uses certain types of personal information about living individuals. This personal data will be processed according to the legal basis of contractual relationships with data subjects, compliance with regulated activities in which the College is engaged or other purposes that are deemed an integral part of the College's charter and charitable objectives, including in the public interest.

4.2 The College only processes personal data for the specific purposes set out in Appendix A of this Policy (or for other purposes expressly permitted by the Act and Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

4.3 The College collects and processes the personal data set out in Appendix C of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (regulatory institutions such as the General Medical Council or National Health Service bodies).

5. Adequate, Relevant and Limited Data Processing

5.1 The College will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up to Date

6.1 The College shall ensure that all personal data collected and processed is kept accurate and up to date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Storage Limitation

7.1 The College shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. Secure Processing

8.1 The College shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. Accountability

9.1 The College, as Data Controller provides a structure that acknowledges the responsibilities and accountability for data protection. This is detailed in Appendix B.

9.2 The College keeps internal records of all personal data collection, holding, and processing, which incorporate the following information:

- The College's name and details, responsible person(s) for data protection (see Appendix B), and any applicable third-party data controllers including auditors, external consultants, software providers and organisations which the College collaborates with to fulfil its' purpose and objectives
- The purposes for which the College processes personal data (see Appendix A);
- Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;
- Details (and categories) of any third parties that will receive personal data from the College;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the College; and
- Detailed descriptions of all technical and organisational measures taken by the College to ensure the security of personal data (refer to the IT Security Policy).

10. Data Protection Impact Assessments

10.1 The College shall carry out a Data Protection Impact Assessment (DPIA) as and when required under the Act and Regulation. The provision of a DPIA shall be overseen by the DPO or Data Controller. A DPIA is required when any new processing activity involves:

- Innovative technology
- Denial of service
- Large-scale profiling
- Biometrics
- Genetic data
- Data matching
- Invisible processing
- Tracking
- Targeting children/vulnerable persons

- Risk of physical harm

10.2 Completion of the DPIA questionnaire will provide a clear indication as to whether a DPIA is required. Advice can be sought from the DPO in completing the questionnaire, if required. Completed questionnaires are reviewed by the DPO.

10.3 Completed DPIAs are reviewed by the DPO and be signed off by the Data Controller.

10.4 DPIAs are to be drafted in accordance with the Guidance issued by the Information Commissioner's Office ("ICO"). Further advice is available from the DPO if required. The fact that a DPIA has been considered shall be recorded in all change control processes, including whether or not a DPIA is required.

10.5 A DPIA will identify the following:-

a. The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data

b. Details of the legitimate interests being pursued by the College, where legitimate interest has been determined as being the lawful basis for processing: a legitimate interest assessment (LIA) is to be complied accordingly.

c. An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed

d. An assessment of the risks posed to individual data subjects

e. Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Act and Regulation.

11. The Rights of Data Subjects

11.1 The Act and Act and Regulation set out the following rights applicable to data subjects:

a. The right to be informed;

b. The right of access;

c. The right to rectification;

d. The right to erasure (also known as the 'right to be forgotten');

e. The right to restrict processing;

f. The right to data portability;

g. The right to object;

h. Rights with respect to automated decision-making and profiling.

11.2 The College is mandated under Article 12 of the UK GDPR to facilitate the rights of data subjects for instance, responding to subject access requests.

11.3 The College is required to respond to all data subject rights requests within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

12. Keeping Data Subjects Informed

12.1 The College shall ensure that the following information is provided - by reference to this Data Protection Policy - to every data subject when personal data is collected:

a. Details of the College including, but not limited to, the identity of any appointed Data Protection Officer;

b. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Appendix A of this Policy) and the legal basis justifying that collection and processing;

c. Where applicable, the legitimate interests upon which the College is justifying its collection and processing of the personal data;

d. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e. Where the personal data is to be transferred to one or more third parties, details of those parties;

f. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 21 of this Policy for further details concerning such third country data transfers).

g. Details of the length of time the personal data will be held by the College (or, where there is no predetermined period, details of how that length of time will be determined (as detailed in Appendix D of this Policy)).

h. Details of the data subject's rights under the Act and Regulation.

i. Details of the data subject's right to withdraw their consent to the College's processing of their personal data at any time.

j. Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Act and Regulation).

k. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.

l. Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 Where the personal data is obtained from the data subject directly, the information above will be provided at the time of collection;

12.3 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a. If the personal data is used to communicate with the data subject, at the time of the first communication; or

b. If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c. In any event, not more than one month after the time at which the College obtains the personal data.

13. Data Subject Access

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the College holds about them. As stated at section 11 above, the College is required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.2 All SAR received must be forwarded to the Data Controller.

13.3 The College will not charge a fee for the handling of SARs. However, the College reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 If a data subject informs the College that personal data held by the College is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. Erasure of Personal Data

15.1 Data subjects may request that the College erases the personal data it holds about them in the following circumstances:

a. it is no longer necessary for the College to hold that personal data with respect to the purpose for which it was originally collected or processed;

b. the data subject wishes to withdraw their consent to the College holding and processing their personal data;

c. the data subject objects to the College holding and processing their personal data (and there is no overriding legitimate interest to allow the College to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);

d. the personal data has been processed unlawfully;

e. the personal data needs to be erased for the College to comply with a legal obligation

15.2 Unless the College has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the College ceases processing the personal data it holds about them. If a data subject makes such a request, the College shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1 The College processes personal data using automated means to ensure compliance with environmental legislation.

17.2 Where data subjects have given their consent to the College to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the College and the data subject, data subjects have the legal right under the Act and Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

17.3 To facilitate the right of data portability, the College shall make available all applicable personal data to data subjects in one of the following formats:

a. CSV files;

b. PDF files

c. other multimedia, electronic (soft) or hard copy files.

17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the College processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for historical research and statistics purposes.

18.2 Where a data subject objects to the College processing their personal data based on its legitimate interests, the College shall cease such processing forthwith, unless it can be demonstrated that the College's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the College processing their personal data for direct marketing purposes, the College shall cease such processing forthwith.

18.4 Where a data subject objects to the College processing their personal data for historical research and statistics purposes, the data subject must, under the Act and Regulation, 'demonstrate grounds relating to his or her particular situation'. The College is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Exercising Data Subject Rights

19.1 Data subjects can exercise their rights by emailing: dataprotection@mooreclear.com

19.2 Alternatively, by writing to:

Data Protection Officer
Royal College of Pathologists
6 Alie St
London
E1 8QT
or emailing: dpo@rcpath.org

20. Data Security

20.1 In accordance with the Data Protection Act 2018 and UK GDPR, we are committed to taking appropriate technical and organisational measures to protect your personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. When you provide your personal data through our websites, this information is transmitted across the internet securely using high-grade encryption.

20.2 The data that we collect from you will be processed at our servers in the UK. It may also be processed by organisations operating in the European Economic Area (EEA) that College has instructed. If your data needs to be transferred outside of the EEA, or to a country that has not been granted a finding of adequacy by EC, we will transfer your data using 'appropriate safeguards' i.e. Binding Corporate Rules (BCR) or Standard Contract Clauses (SCC) (also known as Model Contract Clauses) etc., or we will seek your consent, on a case-by -case basis, and where appropriate to do so.

21. Data Protection Measures

21.1 The College shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a. Appropriate technical and other security measures to safeguard personal information will be taken. These are detailed in the College's IT Security Policy – information for users and the College's e-mail retention policy.

b. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded.

c. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

d. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail or an equivalent postal service;

e. No personal data may be shared informally and if an employee, volunteer, agent, sub-contractor, or other party working on behalf of the College requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Controller

f. Personal data may only be transferred to devices belonging to agents, volunteers, contractors, or other parties working on behalf of the College where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Act and Regulation (which may include demonstrating to the College that all suitable technical and organisational measures have been taken);

g. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

h. No personal data may be transferred to agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Data Controller.

22. Organisational Measures

22.1 The College shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a. All employees, volunteers, agents, contractors, or other parties working on behalf of the College shall be made fully aware of both their individual responsibilities and the College's responsibilities under the Act and Regulation and under this Policy, and shall be provided with a copy of this Policy;

b. Only employees, agents, sub-contractors, or other parties working on behalf of the College that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the College;

c. All employees, volunteers, agents, contractors, or other parties working on behalf of the College handling personal data will be appropriately trained to do so;

d. All employees, volunteers, agents, contractors, or other parties working on behalf of the College handling personal data will be appropriately supervised;

e. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f. The performance of those employees, volunteers, agents, contractors, or other parties working on behalf of the College handling personal data shall be regularly evaluated and reviewed;

g. All employees, volunteers, agents, contractors, or other parties working on behalf of the College handling personal data will be bound to do so in accordance with the principles of the Act and Regulation and this Policy by contract;

h. All agents, contractors, or other parties working on behalf of the College handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the College arising out of this Policy the Act or the Regulation;

i. Where any agent, contractor or other party working on behalf of the College handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the College against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

23. Automated Decision-Making

23.1 In the event that the College uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Act and Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the College.

The right described in above does not apply in the following circumstances:

a. the decision is necessary for the entry into, or performance of, a contract between the College and the data subject;

b. the decision is authorised by law; or

c. the data subject has given their explicit consent.

24. Profiling

24.1 Where the College uses personal data for profiling purposes, the following shall apply:

a. Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b. Appropriate mathematical or statistical procedures will be used;

c. Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented;

d. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

25. International Transfer of Data

25.1 All exports of personal data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the UK GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

25.2 The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions apply:

- Adequacy decision
- Standard contract clauses (otherwise referred to as 'Model contract clauses')
- Binding corporate rules ("BCR")
- International Agreements
- Derogation e.g. transfers made with the consent of the data subject

25.3 In the absence of an adequacy decision, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has consented explicitly to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

26. Data Breach Notification

26.1 All personal data breaches must be reported immediately to the DPO.

26.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the College must ensure that the Information Commissioner's Office is informed of the breach without delay, taking advice as necessary from the DPO, and in any event, within 72 hours after having become aware of it.

26.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 24.2) to the rights and freedoms of data subjects, the College must ensure that all affected data subjects are informed of the breach directly and without undue delay, taking advice as necessary from the DPO.

26.4 Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the DPO (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the College to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

27. General Training

27.1 The College is responsible for ensuring that all of its employees, volunteers, associates, interns and contractors are aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is processed only in line with the College's procedures.

27.2 To this end, the College shall ensure that all of its employees are given appropriate and relevant training.

28. Disciplinary Action

28.1 All staff are to adhere to this policy and its intent. Failure to do so may result in disciplinary action being taken. Such action might include written or verbal warnings or instant dismissal in circumstances that amount to gross misconduct.

28.2 The College reserves the right to take appropriate disciplinary action against contractors and self-employed service providers who fail to comply with this policy. Such actions include, but are not limited to, the termination of any contract with College.

29. Implementation of Policy

29.1 This Policy shall be deemed effective as of [insert date]. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date. The Policy shall be reviewed every three years and in event of significant changes to the Act and Regulation.

Document Owner	Director of Corporate Services	
Approved By	Data Compliance Team	31/1/22
	Trustee Board	10/3/22
Date for Review	31/12/24	
Version	1	

APPENDIX A Purposes for processing personal data **Date: January 2022**

The Royal College of Pathologists exists to promote excellence in the practice of pathology and to be responsible for maintaining standards through training, assessments, examinations and professional development, to the benefit of the public. It was incorporated in 1962, received its Royal Charter in 1970 (Company No RC000127) and is a registered charity (No. 261035). The College is governed by a trustee board. It:

- provides the infrastructure to support training in the pathology specialties
- operates a quality-assured Continuing Professional Development (CPD) scheme, including an online CPD portfolio facility
- provides advice on establishing, approving and maintaining training programmes
- approves educational job descriptions and maintains a network of specialty advisors
- has committees that steer the direction and offer advice to members of all the pathology specialties
- conducts examinations for scientists and doctors wishing to specialise
- provides ready access to the public perspective on pathology through the Lay Advisory Committee
- organises conferences, scientific meetings and academic activities
- collects workforce data and lobbies the UK governments on workforce issues
- proactively approaches the UK governments and independent healthcare providers on pathology issues
- distils guidance from government and other organisations, and publicises this to members
- advises NHS and similar organisations, the independent sector and the public
- provides a conduit for academic and research funding for studentships and fellowships

- provides monitoring of equality, diversity and inclusion of College members and staff to give reports and guidance on such matters to employers and individuals

APPENDIX B– College data protection responsibilities Date: January 2022

The College maintains the following structure in order to meet its responsibilities for the Act and Regulation as well as operational management of data processing. This work and related policies will feed into the Governance Committee with responsibility for managing policy and risk. The approval of policy will be in line with standard policy approvals through the Governance Committee and Trustee Board.

The Senior Management Team

The Senior Management Team with responsibility for maintaining agreed processes and practices within their areas of management. This comprises:

- Chief Executive with responsibility for directly reporting to the Trustee Board on compliance and risk management
- Director of Corporate Services (designated as Data Controller) with responsibility for management of the Data Compliance team and responsible for operational guidance and management systems for data protection.
- Director of Communications with responsibility for oversight of marketing activities with regard to compliance with the Act and Regulation
- Director of Learning
- Director of Professionalism
- Head of IT with responsibility for maintaining secure systems and processes through IT security policies
- HR Manager with responsibility for ensuring training and awareness is carried out for employees and disciplinary policies related to employee's compliance with the policy, The Act and the Act and Regulation

Data Protection Officer

The appointment of an external, professionally qualified DPO to support this policy. The DPO will, among other things, provide advice and guidance on the following:

- policies, procedures and record keeping

- risk assessing personal data breaches and notifications to the ICO and data subjects
- responses to data subject rights requests
- training and staff awareness programmes as required
- advice to the College on changes in legislation or best practice

Data Compliance Team

A team will be drawn from the College staff team, and DPO, with management oversight and responsibility for operational processes and maintenance of data protection policies and activities.

APPENDIX C - PERSONAL DATA **Date: January 2022**

The following data may be collected, held and processed:

1. For members and prospective members:
    a. Any given names, surname and title
    b. Address details for home and work with preferred contact address
    c. Email address for receipt of email correspondence
    d. Telephone numbers: work, home and mobile
    e. Bank account details
    f. Professional work, training and examination details
    g. Special category data
2. For staff:

a. Personal contact details such as name, title, home address, telephone numbers, and personal email addresses
b. Date of birth
c. Special category data
d. Gender
e. Next of kin and emergency contact information
f. National Insurance number
g. Bank account details, payroll records and tax status information
h. Salary, annual leave, pension and benefits information
i. Start date
j. Location of employment or workplace
k. Copy of passport or driving licence
l. Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process.
m. Employment records (including job titles, work history, working hours, training records and professional memberships)

n. Remuneration history

o. Performance information

p. Disciplinary and grievance information

q. CCTV footage and other information obtained through electronic means such as swipecard records

r. Information about your use of our information and communications systems

s. Photographs

The Royal College of Pathologists
Pathology: the science behind the cure

APPENDIX D - Retention Table	**Date: January 2022**
Role	**Responsibility**
Data Controller	To ensure that the collection, retention and destruction of all personal data by each department is carried out according to the requirements of the UK GDPR.
Chief Executive	To ensure that all financial records, including accounting and tax records are retained for no longer than 7 years. To ensure that all personal data stored is not kept for longer than necessary following the below guidelines: 1- Member's data if lapsed should not be kept any longer than 10 years. 2- Members' data is deleted once a period to bring a legal claim for any reasons against the College is lapsed To ensure that all relevant statutory and regulatory records are retained for statutory limitation periods. (with the exception of the aforementioned records listed above).
HR & Development Manager	To ensure that all HR records are retained no longer than 6 years in total. Any settlement agreement between an employer and employee is kept in perpetuity
Chief Executive	To ensure that all Health and Safety records are retained in accordance to the College's Public Liability Insurance policy (normally 40 years).
Director of Communications	To ensure that appropriate consent is obtained to use photographs and video footage.
Director of Corporate Services	To ensure that all personal data involved in the governance of the College are kept for no longer than necessary.
Director of Learning	To ensure all current and previous learners' data including their exam papers are not kept beyond: 1- When they can appeal against a decision 2- When they can continue their academic progress 3- When they can bring a legal claim against the College

Director of Professionalism	To ensure members' professional data such as CPD records are not kept: 1- Once the membership is lapsed and is not renewed 2- Once the member is disqualified from practice and profession as a pathologist or a medical practitioner
Director of Learning (responsible for International Department)	To ensure that personal data that is processed outside of the UK has sufficient organisational and technical measures to protect data subjects' rights and that personal data processed from data subjects outside of the UK is similarly protected.