Data Protection & Privacy Policy

Contents

Document Key Data

Owner:	Vice Principal Finance & Resources	Approved by:	Board
Review interval:	3 years	Approved on:	3 April 2025
Date of next review:	April 2028	Post to website:	Yes

Data Protection & Privacy Policy

1. Introduction

1.1 This Policy sets out the obligations of Richmond & Hillcroft Adult & Community College (the College) regarding data protection and the rights of, inter alia, learners, staff, volunteers and visitors ("data subjects") in respect of their personal data under the Data Protection Act 2018 and the associated UK GDPR including any subsequent amendments.

1.2 The UK GDPR 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, in particular 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.

1.3 This Policy sets out the College's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the College, its employees, agents, contractors, or other parties working on behalf of the College.

1.4 The College is committed not only to the letter of the law, but also to the spirit of the law and 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.

2. The Data Protection Principles

2.1 This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

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

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

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

2.1.4 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 it is processed, is erased, or rectified without delay.

2.1.5 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 UK GDPR in order to safeguard the rights and freedoms of the data subject.

2.1.6 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.

3. The Rights of Data Subjects

3.1 The Data Protection Act 2018 and the UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

2.1.7 The right to be informed (Part 12).

2.1.8 The right of access (Part 13);

2.1.9 The right to rectification (Part 14);

2.1.10 The right to erasure (also known as the 'right to be forgotten') (Part 15);

2.1.11 The right to restrict processing (Part 16);

2.1.12 The right to data portability (Part 17);

2.1.13 The right to object (Part 18);

2.1.14 Rights with respect to automated decision-making and profiling (Parts 19 and 20); and

2.1.15 The right to complain to the Information Commissioner's (ICO) (Part 30)

4. Lawful, Fair, and Transparent Data Processing

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

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

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

4.1.5 The 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 data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data 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, in particular where the data subject is a child.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless UK law prohibits them from doing so);

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by UK law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

4.2.5 The processing relates to personal data which is clearly made public by the data subject;

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.7 The processing is necessary for substantial public interest reasons, on the basis of UK law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of UK law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, 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, on the basis of UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR based on UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

5.1 The College collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 The College only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the UK GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the College uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

6.1 The College will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The College shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The College shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 The College will:

- identify records that it is appropriate to archive and centrally manage the archiving
- consider issues such as cost, space utilisation, long term quality of storage, the medium of storage and accessibility when determining how to archive materials
- regularly review materials that are archived and dispose of materials that it is no longer appropriate to retain.

8.4 For full details of the College's data retention periods for specific personal data types held by the us, please refer to Appendix 1.

9. Secure Processing

9.1 The College shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

10.1 The College's Data Protection Officer is GDPR Sentry Limited, Unit 434 Birch Park, Thorp Arch Estate, Wetherby, West Yorkshire, LS23 7FG, 0113 804 2035, support@gdprsentry.com

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the College's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation. The Vice Principal Finance & Resources will be the point of contact within RHACC relating to data protection related issues.

10.3 The College shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of The College, its Data Protection Officer, and any applicable third-party data processors;

10.3.2 The purposes for which The College collects, holds, and processes personal data;

10.3.3 Details of the categories of personal data collected, held, and processed by The College, and the categories of data subject to which that personal data relates;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.5 Details of how long personal data will be retained by the College (please refer to our Data Retention Policy); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the College to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The College shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The College's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the College; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The College shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

12.1.2.1 if the personal data is used to communicate with the data subject, when the first communication is made; or

12.1.2.2 if the personal data is to be transferred to another party, before that transfer is made; or

12.1.2.3 as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the College including, but not limited to, the identity of its Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

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

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

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

12.2.6 Details of the data subject's rights under the UK GDPR;

12.2.7 Where the personal data is to be transferred to a third party that is located in a territory without an adequacy agreement as approved by the UK Government, details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);

12.2.8 Details of data retention;

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

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR);

12.2.11 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; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the College holds about them, what it is doing with that personal data, and why.

13.2 All subject access requests should be made to DPO@rhacc.ac.uk.

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

13.5 The College does not charge a fee for the handling of normal SARs. 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 Data subjects may have the right to require the College to rectify any of their personal data that is inaccurate or incomplete.

14.2 Where such rectification is possible, The College shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the College of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

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

15. Erasure of Personal Data

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

15.1.1 It is no longer necessary for The College to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to The College holding and processing their personal data;

15.1.3 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 the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for The College to comply with a particular legal obligation; or

15.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

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. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's 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 restricts processing the personal data it holds about them. If a data subject makes such a request, The College shall in so far as is possible ensure that the personal data is only stored and not processed in any other fashion.

16.2 If the College is required to process the data for statutory purposes or for reasons of legal compliance, then the College shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

16.3 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. Such processing is carried out by, inter alia, our management information system, our human resources systems and our payroll system.

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 right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the College processing their personal data based on performing a task in the public interest, the College's legitimate interests, or direct marketing (including profiling)

18.2 Where a data subject objects to the College processing their personal data, the College shall cease such processing immediately, unless it can be demonstrated that the College's grounds for such processing override the data subject's interests, rights, and freedoms, or that 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 immediately.

18.4 Where a data subject objects to the College processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, "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. Automated Decision-Making

19.1 In the event that that College uses automated decision-making processes, the College shall notify data subjects of its' intentions to use such processing.

19.2 Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the UK GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the College.

19.3 The right described in Part 19.2 does not apply in the following circumstances:

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

19.3.2 The decision is authorised by law; or

19.3.3 The data subject has given their explicit consent.

20. Profiling

20.1 The College uses personal data for profiling purposes. These purposes relate to helping student maximise achievement and monitor staff performance.

20.2 When personal data is used for profiling purposes, the following shall apply:

20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

20.2.2 Appropriate mathematical or statistical procedures shall be used;

20.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

21. Personal Data Collected, Held, and Processed

21.1 The College uses a wide range of personal data across many processes. If you wish to view the complete lists of categories of personal data we process please contact our Data Protection Officer (dpo@rhacc.ac.uk)

22. Data Security - Transferring Personal Data and Communications

22.1 The College shall ensure that the appropriate measures are taken with respect to all communications and other transfers involving personal data:

22.1.1 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

22.1.2 The College will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered.

22.1.3 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;

22.1.4 Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the e-mail.

22.1.5 Where personal data is to be transferred in removal storage devices, these devices

shall be encrypted. The use of unencrypted removable storage devices is prohibited by The College.

23. Data Security - Storage

23.1 The College shall ensure that the following measures are taken with respect to the storage of personal data:

23.1.1 All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption;

23.1.2 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;

23.1.3 All personal data relating to the operations of The College, stored electronically, should be backed up on a regular basis

23.1.4 Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Acceptable Use policy of the College. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information.

24. Data Security - Disposal

24.1 When 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. For further information on the deletion and disposal of personal data, please refer to the College's Data Retention Schedule at Appendix 1.

25. Data Security - Use of Personal Data

25.1 The College shall ensure that the following measures are taken with respect to the use of personal data:

25.1.1 No personal data may be shared informally and if an employee, 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 Director of Finance and Resources;

25.1.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of The College or not, without the initial authorisation of the Director of Finance and Resources;

25.1.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

25.1.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

25.1.5 Where personal data held by the College is used for marketing purposes, it shall be the responsibility of the Head of Marketing to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

26. Data Security - IT Security

26.1 The College shall ensure that appropriate measures are taken with respect to IT and information security. Please refer to the College's IT Acceptable Use Policy for more detail.

27. Organisational Measures

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

27.1.1 All employees, agents, contractors, or other parties working on behalf of The College shall be made fully aware of both their individual responsibilities and our responsibilities under the UK GDPR and under this Policy, and shall have free access to a copy of this Policy;

27.1.2 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;

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

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

27.1.5 All employees, agents, contractors, or other parties working on behalf of the College handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

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

27.1.7 All personal data held by the College shall be reviewed periodically, as set out in para 8.3;

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

27.1.9 The contravention of these rules will be treated as a disciplinary matter.

27.1.10 All employees, 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 UK GDPR and this Policy by contract;

27.1.11 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 and the UK GDPR; and

27.1.12 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.

28. Transferring Personal Data to a Country without an adequacy decision

28.1 The College may from time to time transfer ('transfer' includes making available remotely) personal data to countries without a suitable adequacy decision from the UK Government.

28.2 The transfer of personal data to a country without an adequacy decision shall take place only if one or more of the following applies:

28.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK Government has determined ensures an adequate level of protection for personal data;

28.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK Government compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

28.2.3 The transfer is made with the informed consent of the relevant data subject(s);

28.2.4 The transfer is necessary for the performance of a contract between the data subject and the College (or for pre-contractual steps taken at the request of the data subject);

28.2.5 The transfer is necessary for important public interest reasons;

28.2.6 The transfer is necessary for the conduct of legal claims;

28.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

28.1.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

29. Data Breach Notification

29.1 All personal data breaches must be reported immediately to the College via the Director of Finance and Resources who will report it to UK GDPR Sentry, Data Protection Officer.

29.2 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 Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach

without delay, and in any event, within 72 hours after having become aware of it.

29.3 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 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

29.4 Data breach notifications shall include the following information:

29.4.1 The categories and approximate number of data subjects concerned;

29.4.2 The categories and approximate number of personal data records concerned;

29.4.3 The name and contact details of the College's data protection officer (or other contact point where more information can be obtained);

29.4.4 The likely consequences of the breach;

29.4.5 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.

30. Monitoring and Reporting

30.1 We will regularly review and update this Data Protection Policy to ensure its continued effectiveness and compliance with applicable data protection laws. We will monitor our data protection practices to verify compliance and address any issues identified.

30.2 For any questions or concerns regarding the processing of personal data or this Data Protection Policy, please contact our Data Protection Officer at dpo@rhacc.ac.uk.

30.3 If you or another data subject are not satisfied with how the College is processing personal data, a complaint can be made to the Information Commissioner. You can find out more about your rights under data protection legislation from the Information Commissioner's Office website.

31. Implementation of Policy

31.1 This Policy shall be deemed effective until further notice**.** No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Appendix 1- Records Retention Period

Sets out guidelines for the retention period of records created and maintained by the College in the course of its business. The appendix refers to all information regardless of the media in which it is stored. Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the Data Protection Act 2018 and the Freedom of Information Act 2000.

1. Staff Related

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + Action at the end of the Retention Period	Location
1.1	Staff Personnel files	Data Protection and HR Policies and Procedures	Yes	Both	Termination + 10 years	Limitation period for litigation; Provision of references	Head of HR SHRED/ DESTROY	HR Office
1.2	Timesheets; Wages and salary records	Financial Regulations	Yes	Both	6 years from the last date of employment	Period of possible inspection	Payroll Manager SHRED/ DESTROY	Finance Office
1.3	Recruitment including application forms and interview notes (Where applicant is success this becomes part of their record)	Recruitment and Selection Policy	Yes	Both	Date of Interview + 6 months (Unless applicant is informed and agrees that we would like to retain records for consideration for future vacancies Or Bank staff.)	Monitoring and conducting of the recruitment process	Head of HR SHRED/ DESTROY	HR Office

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + Action at the end of the Retention Period	Location
1.4	Advertising of vacancies	Recruitment and Selection Policy	No	Electronic/Paper based	6 years	Business	Head of HR	HR Office
1.5	Pre-employment vetting information (inc. DBS checks)	DBS Guidance & Procedure	Yes	Paper based	Date of check + 6 months.	DBS regulations	Head of HR SHRED	HR Office
1.6	Disciplinary proceedings							
1.6a	Stage 1 - Oral warning	Disciplinary Procedure	Yes	Paper based	Date of warning + 6 months Live After spent remains on file as per 1.1	Acas Code Guidance	Head of HR SHRED	HR Office
1.6b	Stage 2 – Written warning	Disciplinary Procedure	Yes	Paper based	Date of warning + 12 months Live After spent remains on file as per 1.1	Acas Code Guidance	Head of HR SHRED	HR Office
1.6c	Stage 3 – Final written warning	Disciplinary Procedure	Yes	Paper based	Date of warning + 18 Months Live After spent remains on file as per 1.1	Acas Code Guidance	Head of HR SHRED	HR Office
1.6d	Case not found after disciplinary investigations	Disciplinary Procedure	Yes	Paper based	Remains on file as per 1.1	Acas Code Guidance	Head of HR	HR Office

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + Action at the end of the Retention Period	Location
1.7	Income tax and NI Returns; Correspondence with Tax Office	Financial Regulations & Procedures	Yes	Electronic/Paper based	6 years after the end of the financial year to which the records relate	Period of possible inspection	Payroll Manager SHRED	HR Office
1.8	Statutory parental pay records and calculations	Parental Leave Policy	Yes	Paper based	6 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations (1986)	Payroll Manager SHRED	HR Office
1.9	Statutory Sick Pay records and calculations	Sickness absence Policy	Yes	Paper based	6 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations (1982)	Payroll Manager SHRED	HR Office
1.10	Occupational health records, health surveillance and environmental monitoring (affecting health)	Sickness absence Policy; Stress Policy	Yes	Both	10 years		Head of HR SHRED/DESTROY	HR Office
1.11	Records relating to accident/injury at work	Health & Safety Policy	Yes	Both	Date of incident + 10 years	Management of health and safety include to influence the policy Management of civil claims	Head of HR SHRED/DESTROY	HR Office

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + Action at the end of the Retention Period	Location
1.12	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995		Yes	Both	Current year + 40 years	Scheme requirements	Head of HR SHRED	HR Office/ Finance Office

2. Health and Safety

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
2.1	Accident Reporting	H&S Policy	No	Both	Date of incident + 10 years for adults Learners under 18 have until their 25th birthday to make a claim for negligence	Purposes of Civil Claims	Head of Estates SHRED/DESTROY	Estates Office
2.2	COSHH	H&S Policy	No	Both	Current year + 10 years	Development and monitoring of Health and Safety policies and procedures	Head of Estates SHRED/DESTROY	Estates Office
2.3	Incident reports	Disaster Management & Business Continuity Plan	Yes	Both	Current year + 20 years	Development and monitoring of Health and Safety policies and procedures Management of Business Continuity Plans	Head of Estates SHRED/DESTROY	Executive Office
2.4	Policy Statements	H&S Policy	No	Both	Date of Expiry + 1 year	Development and monitoring of Health and Safety policies and procedures	Head of Estates	Estates Office

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
2.5	Risk Assessments	H&S Policy	No	Both	Current year + 3 years	Development and monitoring of Health and Safety policies and procedures	Head of Estates	Estates Office
2.6	Fire log books	H&S Policy	No	Paper based	Current year + 6 years	Development and monitoring of Health and Safety policies and procedures	Head of Estates	Estates Office

3. Governance and Management

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
3.1	Legal Framework	Instruments & Articles of Governance	No	Electronic & Paper	Life of College and then archived for future iteration college/history	Legal Requirement	Clerk ARCHIVE	Shared Drive Paper copies in Clerk's Office
3.2	Signed Minutes		No	Electronic	Permanent	To look back and see why decisions were made in the future and history	Clerk ARCHIVE	Signed paper copies – not applicable Electronic copies: Shared Drive GVO Portal
3.3	Agendas		No	Electronic	Date of Meeting + 6 years	To look back and see why decisions were made in the future and history	Clerk SHRED	Electronic copies: Shared Drive GVO Portal
3.4	Reports		No	Electronic	Date of report + 6 years	To look back and see why decisions were made in the future and history	Clerk ARCHIVE	Electronic copies: Shared Drive GVO Portal

4. Management

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
4.1	Minutes of the Senior and Executive Management		Yes	Electronic	Date of meeting + 6 years	Legitimate Interest and to manage the college	Executive PA DESTROY	Shared Drive
4.2	Strategic Development Plans		No	Electronic	Permanent	Legitimate Interest and to manage the college	Clerk	Clerk's Office

5. Audit

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
5.1	Internal and External Audit Reports	Financial Regulations	No	Electronic	6 years after publication		Vice Principal Finance & Resources DESTROY	Shared Drive

6. Insurance Management

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
6.1	Insurance Policies – Employer's Liability	Financial Regulations	No	Paper	Minimum of 6 years and a maximum of 40 years, subject to contracts	Management and monitoring of insurance claims	Head of Finance SHRED	Finance Office
6.2	Records of insurance claims – damage to property	Financial Procedures Damage, Loss & Theft Procedure	Yes	Both	10 years after settlement of claim	Management and monitoring of insurance claims	Head of Finance SHRED/DESTROY	Finance Office
6.3	Records of insurance claims – personal injury	Financial Procedures H&S Policy	Yes	Both	10 years after settlement of claim	Management and monitoring of insurance claims	Head of Finance SHRED/DESTROY	Finance Office

7. Student Records

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
7.1	Individual Learner Records including enrolment form and withdrawal/transfer information; change of student details	Data Protection	Yes	Both	Termination of the relationship with the student + 6 years (including records relating to a student who has withdrawn from the organisation)	Funding body audit purposes	Head of Admissions SHRED/ DESTROY	REMS & Learner Services Office
7.2	Learner Support Fund (LSF) Records		Yes	Both	Current year + 6 years	Funding body audit purposes	Head of Admissions SHRED/ DESTROY	REMS & Learner Services Office
7.3	Applications for Admission - successful students		Yes	Both	End of relationship with student + 1 year		Head of Admissions SHRED/ DESTROY	REMS & Learner Services Office
7.4	Applications for Admission - unsuccessful students		Yes	Both	Resolution of any appeal + 1 year		Head of Admissions SHRED	Learner Services Office

7.5	Records relating to the registration of individual students on programmes and examination results	Data Protection Policy; Freedom of Information	Yes	Both	Termination of relationship with student +3 years		Exams Manager SHRED/ DESTROY	Exams Office
7.6	Records documenting individual attendance at examinations and handling requests for mitigating circumstances	Data Protection Policy; Freedom of Information	Yes	Paper only	Current academic year + 1 year to point of certification		Exams Manager SHRED/ DESTROY	Exams Office
7.7	Pass lists/awards lists	Data Protection Policy; Freedom of Information	Yes	Both	Issue of list + 3 years		Exams Manager SHRED/ DESTROY	Exams Office
7.8	Records relating to the handling of individual student requests for personal data including statements/results/ transcripts	Data Protection Policy; Freedom of Information	Yes	Both	Last action on request + 1 year		Exams Manager SHRED/ DESTROY	Exams Office
7.9	Assessment and Verification records including records relating to the academic progress of individual student (including any action taken to deal with unsatisfactory progress); details relating to submission and marking of coursework	Assessment Policy	Yes	Both	Termination of relationship with student + 3 years		Tutors and Program Leaders SHRED/ DESTROY	Staff work areas

7.10	Records relating to disciplinary action (also applies to Appeals)	Student Disciplinary Procedure	Yes	Both	Last action + 3 years		Tutors and Program Leaders SHRED/ DESTROY	Quality Office
7.11	Records relating to fitness to study action (also applies to Appeals	Fitness to Study Procedure	Yes	Both	Last action + 3 years		Tutors and Program Leaders SHRED/DESTROY	Quality Office
7.12	Records relating to formal student complaints (complaint not dealt with through Complaints procedure)	Complaints Procedure	Yes	Both	Last action + 6 years Last action + 3 years		Executive PA SHRED/ DESTROY	Executive Office
7.13	Special Educational Needs files, reviews and individual education plans	Equality and Diversity Policy	Yes	Paper	Termination of relationship with student + 6 years For learners under 18, records should be retained until their 25th birthday as a minimum	Special Educational Needs and Disability Act 2001 Section 1	Head of School SHRED unless any legal action pending	Foundation Learning School
7.14	Advice & Guidance Documentation	Information, Advice & Guidance Policy	Yes	Both	Termination of relationship with student + 3 years		Learner Advice and Guidance Manager SHRED/ DESTROY	IAG Office

8. Child and Vulnerable Adult Protection

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
8.1	Child and vulnerable adult protection files	Safeguarding Policy	Yes	Electronic	Termination of relationship with student or for learners under 18, until their 25th birthday	Education Act 2002, s175, related guidance "Safeguarding Children in Education," September 2024	Vice Principal – Quality &Curriculum DESTROY	Vice Principal's office
8.2	Allegation of a child and vulnerable adult protection nature against a member of staff, including where the allegation is unfounded	Safeguarding Policy	Yes	Both	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary & Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against teachers and other staff" November 2005	Head of HR SHRED/ DESTROY	HR Office

9. Procurement

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
9.1	Tender records	Financial Regulations	Yes	Paper	6 years after completion of tendering process		Executive PA and Clerk ARCHIVE	Clerk's Office
9.2	Supplier approval	Approved Supplier Procedures	No	Electronic	Current year + 6 years		Head of Finance SHRED	Finance Office
9.3a	Contract records:	Financial Procedures	No	Paper	Contract completion date + 6 years (Longer for buildings)		Head of Finance SHRED	Finance Office
9.3b	Contract monitoring records	Financial Procedures	No	Paper	Current year + 6 years		Head of Finance	Finance Office

10. Financial Management

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
10.1	Financial records	Financial Regulations and Procedures	No	Both	Current year + 6 years	VAT and Tax Regulations; Limitation Act 1980	Head of Finance SHRED/DESTROY	Finance Office
10.2	Annual Financial Statements	Financial Regulations	No	Both	Permanently		Head of Finance ARCHIVE	Finance Office
10.3	Loans and Grants	Financial Regulations	No	Paper	Date of last payment on loan + 12 years		Head of Finance ARCHIVE	Finance Office
10.4	Risk Register	Financial Regulations Risk Management Policy	No	Electronic	Current year + 6 years		V.P. Finance & Resources DESTROY	Finance Office
10.5	Finance Returns	Financial Memorandum	No	Electronic	Current year + 6 years	VAT and Tax Regulations; Limitation Act 1980	Head of Finance DESTROY	Finance Office

11 Property

	Basic File Description	Related Policy/ Procedure	Data Protection Issues	Electronic/ Paper Based	Retention period	Reason	Responsibility + action at the end of the Retention Period	Location
11.1	Title Deeds		No	Paper	Life of College		Principal ARCHIVE	Principal's Office
11.2	Plans of Buildings		No	Both	Life of College		Head of Estates ARCHIVE	Estates Office
11.3	Maintenance and Contractors	Financial Regulations Approved Suppliers Procedure	No	Both	Current year + 6 years		Head of Finance SHRED/ DESTROY	Finance Office
11.4	Hires	Financial Procedures	No	Paper	Current year + 3 years		Hires & Events Co-ordinator	Events Office

Appendix 2 - Retention Of European Regional Development Fund (Erdf) And Euroepan Social Fund (Esf) Project Files To 2030

Sets out the guidelines for the retention of European Social Fund (ESF) funded projects up to 2030. ESF projects funded through the current round 2014 to 2022 will be governed by similar guidelines with an expectation that records must be retained until 3 years after the European Commission make their final payment for the programme.

All projects in receipt of ERDF and ESF funds need to be aware of their obligations to comply with the European Commission (EC) regulations about preserving documents and preserving an audit trail.

Documents relating to projects supported under 2014-2022 programmes should be retained for a period of three years following the final payment by the European Commission. This means that documents may need to be retained to around 2030.

The following documents must be retained:

A. Contract and claims

- Original ERDF/ESF application form
- Letter of approval / contract
- Evidence to substantiate match funding
    - Confirmation letters
    - Bank statements demonstrating payments received
    - Evidence for in-kind support
- Advance (ESF) and interim claim forms
- Final claim forms
- External auditor's report
- Project Closure Report forms (ESF)
- General Statements of Expenditure
- Any letters from DCLG/DWP/GOL and other responsible authorities
- Sub-contract arrangements

o Service level agreements o Tendering documents o Contracts o Monitoring strategies for delivery partners.

B. Project Records

- Project timetable and programme including modules
- Application / eligibility assessment forms
- List of beneficiaries on the project
- Project register and attendance records
- Project start and finish dates
- In and end year monitoring
- Records of achievement
- Follow-up information

C. Individual Beneficiary Records (ESF)

- Application form, including a signed declaration
- Terms and conditions of training, including individual project / training programme
- Individual attendance records including start and end date
- Suitability / assessment records
- Monitoring beneficiary progress
- Work experience records if relevant
- Copies of certificates gained
- Course evaluation forms by beneficiary
- Beneficiary follow-up form

D. Financial Records

All items on claims and project closure reports supported by source documentation:

- Working papers to show how the claim was compiled
- Staff costs - detailed salary records
- Beneficiary costs
- Other costs
- Match funding
- Invoices and payment receipts (originals)
- Accounts and bank statements
- Organisation / college based unit cost calculation (HEIs only)
- Apportionment methodology, i.e. letters to and from GOL stating methodology and agreement to it.

It is good practice to ensure that all financial information, e.g. invoices etc. are stored together on the relevant project files.

E. Publicity

All evidence showing EC publicity requirements were adhered to:

- Leaflets
- Pamphlets
- News articles
- Examples of Letterhead with correct logo
- Print outs of web pages demonstrating use of logo
- Retained photograph of any billboards with logo (ERDF)

Additionally, projects must be able to demonstrate a clear audit trail when required. Audit trails should enable inspections to verify that:

- there is evidence to support the claim and that expenditure has been incurred in a proper manner;
- there is sound financial management;

- there is compliance with EC regulations and the requirements of their contract;
- interim and project closure report entries are supported by evidence of expenditure; and,

- the project represents value for money.

F. Retention of electronic documents

Where documents exist in electronic version only, the supporting computer systems must be secure and comply with national legal requirements - e.g. systems that comply with the requirements of Customs & Excise and Inland Revenue. Electronically stored documents and supporting systems must be relied upon for audit purposes.

Where original documents have been copied in order to comply with these conditions accepted data carriers include the following:

- photocopies of original documents;
- microfiches of original documents;
- electronic versions of original documents on optical data carriers (such as DVD, hard disk or magnetic disk).

Each document should be certified as conforming to the original document, along the lines of the example below. This is the minimum requirement and projects may add to this declaration or include additional procedures in line with their organisations policies should they wish to do so.

I certify that this is a true copy of the original document
Signed ..... Date.....
Position in organisation.....
Name of organisation.....

Projects must keep the electronic copy of the document for the same duration as required for paper copies.

Equality Impact Assessment: Initial Screening (Stage 1)

Name of Policy or Practice: Data Protection & Privacy Policy

Person/ Team/ Department Responsible: Vice Principal Finance & Resources

Date of Assessment: 4 March 2025

Consider the three aims of the public equality duty:

- To eliminate discrimination
- To advance equality of opportunity
- To foster good relations

Protected Characteristics:

Age, Disability, Gender Reassignment, Race, Religion or Belief, Sex, Sexual Orientation, Marriage & Civil Partnership, Pregnancy & Maternity

Q1) What is the purpose of the policy, decision or practice	***Outline to learners, staff and visitors to the College their data privacy and protection rights***

2) Who is affected by the initiative? Does the initiative make a positive contribution to equality and diversity in the College? Or is it equality neutral i.e. no particular effect on anyone group? ***All learners, staff and visitors are potentially impacted by the policy. The policy does not have an impact on any particular group. The policy is equality neutral.***
3) Is there the potential for there to be a negative impact on one or more of the Equality groups as a result of this initiative? If so what groups may be effected and why? Or is it equality neutral? ***The policy is equality neutral.***
4) Has anyone complained about the policy or initiative? ***No***
5) Is the impact of the initiative significant enough to warrant a more detailed assessment? ***No*** If yes please circle priority rating for assessment: High Medium Low