

# GDPR Data Protection Policy

HARROW, RICHMOND AND UXBRIDGE COLLEGES POLICY AND PROCEDURES



<b>Policy No:</b>	D03
<b>Subject:</b>	Data Protection Policy
<b>Last approved:</b>	July 2025
<b>Effective date:</b>	July 2025
<b>Review date:</b>	July 2026
<b>Person responsible:</b>	Chief Technology Officer
<b>Approved by:</b>	Technical Infrastructure Board
<b>For action by:</b>	All Staff
<b>For information to:</b>	All Staff

## 1. Background

- 1.1 This document sets out the Data Protection Policy for HRUC (the College).
- 1.2 The aim of this policy is to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their duties.
- 1.3 This policy sets out how we comply with our data protection obligations set out in the UK General Data Protection Regulation (the “UK GDPR”) and the Data Protection Act (“DPA”) 2018 and seek to protect the personal data of all individual stakeholders we interact with who may come into contact with us.

## 2. Scope

- 2.1 The Data Protection Policy applies to all staff and members of HRUC. For clarity, the term staff means anyone working in any context for the College at any level or grade (whether permanent, fixed term or temporary) and including employees, retired but active members and staff, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of College committees. The term member includes learners and alumni of the College when they are handling or processing personal information on behalf of the College, except when they are acting in a private or external capacity.

- 2.2 The term “Personal Data” referred to throughout this document applies to personal information relating to any living individual which is stored at the College either in electronic or paper format. The individual may be referred to as the ‘Data Subject’.
- 2.3 Learner Records and Learner Services are responsible for securely maintaining the Personal Data of all learners enrolled at the College.
- 2.4 The Human Resources department is responsible for securely maintaining the Personal Data of all persons working at the College, including employees, agency staff and voluntary workers. This department will:
- a) Ensure that Data Protection obligations are reflected in the College’s Disciplinary Procedures and contracts of employment.
  - b) Ensure that all staff are aware of the types of personal information that the College will process on them and ask staff to check this information as required.
  - c) Ensure that all obligations outlined within the DBS Code of Practice are adhered to.
  - d) Provide advice to managers and others on the application of the DBS Code of Practice.
  - e) Destroy staff personal data according to the College’s data retention policy.
- 2.5 Whilst all staff and users of personal data have some responsibility for the security of data, IT and MIS staff have an important role in ensuring the security of computerised data. In particular they will:
- a) Be responsible for advising the College on the state of technological development with regard to IT security.
  - b) Provide secure methods of transferring authorised personal data outside the College.
  - c) Back up data on the College’s IT systems and have disaster recovery procedures in place.
  - d) Implement virus detection and hacking preventative measures.
  - e) Through liaison with the appropriate manager, ensure that the College’s business systems are secure and appropriate restrictions on access are in place so that individuals only have access to personal data in which they have a legitimate business interest.
  - f) Require the use of passwords and ensure they are changed regularly.
  - g) Produce and update policies for the use of College IT facilities including email, intranet and internet.
  - h) Investigate breaches of IT security.
  - i) Ensure that data is deleted according to the College’s data retention policy.
- 2.6 Every staff member has an implied duty through their Contract of Employment to comply with the requirements of this Policy. Staff must:
- a) Ensure they keep confidential all Personal Data they collect, store, use and come into contact with during the performance of their duties.
  - b) Not release or disclose any Personal Data outside the College, or internally to staff not authorised to access the Personal Data. To do so they must obtain specific authorisation from their manager or the Data Protection Officer.
  - c) Take all steps to ensure there is no unauthorised access to Personal Data whether by other staff not authorised to access the Personal Data or by people outside the College.
- 2.7 Any individuals or organisations contracted with the College must comply with the requirements of this Policy.

### **3. Definitions**

3.1 Key definitions are at Appendix 1.

## **4. Data Protection Principles**

4.1 The UK GDPR contains six 'Data Protection Principles', set out in Article 5 UK GDPR, stipulating that personal data must be:

- a) Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- b) Collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation')
- c) Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').
- d) Accurate and kept up to date, meaning that every reasonable step must be taken to ensure Personal Data that is inaccurate is erased or rectified as soon as practicable ('accuracy')
- e) Kept for no longer than is necessary for that purpose ('storage limitation')
- f) Processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.2 In addition, the College is also responsible for and must be able to demonstrate compliance with the above principles ('accountability'). This means that the College will:

- inform individuals about how and why we process their personal data, usually by way of a privacy notice;
- be responsible for checking the quality and accuracy of the data;
- regularly review records held to ensure that data is not held longer than is necessary, and that it has been held in accordance with records retention policy;
- ensure that when data is authorised for disposal it is disposed of / deleted appropriately;
- ensure appropriate security measures to safeguard personal data whether it is held in paper files or electronically, and follow the requirements set out in our information security policy at all times;
- share personal data with others only when it is necessary and legally appropriate to do so;
- has set out clear procedures for responding to requests for access to personal data known as subject access requests and other rights exercised by individuals in accordance with the UK GDPR (please see "Part 2: Data Subject Rights Policy" below); and
- report any actual or suspected personal data breaches in accordance with the procedure set out in the Data Breach Notification Policy & accompanying procedure.

4.3 Staff guidelines for data protection are at Appendix 2.

## **5. Individual Rights**

5.1 Individual rights are set out in a separate part of the UK GDPR. In brief, the UK GDPR provides the following rights for individuals:

- a) The right to be informed of how their Personal Data are being used. This right is usually fulfilled by the provision of 'privacy notices' (also known as 'data protection statements' or,

especially in the context of websites, 'privacy policies') which set out how an organisation plans to use an individual's Personal Data, who it will be shared with, ways to complain, and retention policies.

- b) The right of access to their Personal Data
- c) The right to have their inaccurate Personal Data rectified
- d) The right to have their Personal Data erased (right to be forgotten). Individuals have the right to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing.
- e) The right to restrict the processing of their Personal Data pending its verification or correction.
- f) The right to receive copies of their Personal Data in a machine-readable and commonly used format (right to data portability).
- g) The right to object: to processing (including profiling) of their data that proceeds under particular legal basis; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest
- h) The right not to be subject to a decision based solely on automated decision-making using their Personal Data.

5.2 The availability of rights largely depends on the legal justification for processing. The table below summarises when rights are available.

Legal Justification	Right to:				
	Object	Erasure	Automated Decision Making	Rectification	Portability
Consent	X but can withdraw consent	✓	X but can withdraw consent	✓	✓
Contract	X	✓	X	✓	✓
Legal Obligation	X	X	X	✓	X
Vital Interest	X	✓	X	✓	X
Public Task	✓	X	✓	✓	X
Legitimate Interests	✓	✓	✓	✓	X

5.3 More information on managing individual rights requests is available in Part 2.

## 6. Data Quality – Ensuring the Use of Accurate, Up to Date and Relevant Personal Data

- 6.1 Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.
- 6.2 All College staff that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.
- 6.3 All College staff that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and

limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College staff to independently check the Personal Data obtained.

- 6.4 In order to maintain the quality of Personal Data, all College staff that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

## **7. Collection of Personal Data**

- 7.1 The specific conditions contained in Article 6 and 9 of the UK GDPR regarding the fair collection and use of Personal Data will be fully complied with. Data Subjects will be made aware that their information has been collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection through relevant privacy notices. It is important that the lawful basis for processing any Personal Data is determined and documented; under the UK GDPR the lawful basis for processing has an effect on an individual's rights.
- 7.2 In order for the collection of Personal Data to be legal and appropriate for the College to process the information must satisfy at least one of the following conditions:
- a) The Data Subject has given his or her consent.
  - b) The processing is required due to a contract with the data subject.
  - c) It is necessary due to a legal obligation on HRUC.
  - d) It is necessary to protect someone's vital interests (i.e. life or death situation).
  - e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in HRUC.
  - f) It is necessary for the legitimate interests of HRUC or a third party and does not interfere with the rights and freedoms of the Data Subject (this condition cannot be used by the public authorities in performance of their public tasks).
  - g) Is it necessary for a "recognised" legitimate interest" ('RLI') of HRUC or a third party (for example, safeguarding of individuals, assisting the police in the investigation of an alleged offence, making a disclosure to another public body which needs the personal data to perform its public task, etc). Where an RLI applies, the rights and freedoms of the Data Subject need not be balanced against the legitimacy of the relevant interest.
- 7.3 All processing of Personal Data carried out by the College must meet one or more of the conditions above. In addition, the processing of 'special categories' of Personal Data requires extra, more stringent, conditions to be met in accordance with Article 9 of the UK GDPR.
- 7.4 Public authorities are not encouraged to use consent for core activities due to the imbalance in the relationship between the Controller and Data Subject. In such cases it is unlikely that consent could be deemed to be freely given. Therefore, where possible the College should identify alternative justifications for processing which would normally be 'official authority vested in the controller', 'public task', 'legal obligation', 'recognised legitimate interest' or 'contract', in these cases the official authority or relevant part of the contract should be identified.
- 7.5 When collecting data, the College will ensure that the Data Subject:

- a) Clearly understands why the information is needed
- b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.
- d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.
- e) Has received sufficient information on why their data is needed and how it will be used.

## **8. Consent**

- 8.1 Where consent is relied upon as the lawful basis for processing any Personal Data, it must be freely given, specific, informed, unambiguous and able to be withdrawn. Also, how and when the consent was obtained will need to be recorded (and review this over time). Consent will require “clear affirmative action” and the Information Commissioner’s Office (ICO) has noted that there is little difference between “explicit” and “unambiguous”. Silence, pre-ticked boxes or inactivity will not constitute consent.
- 8.2 The College will also have to tell individuals that they have the right to withdraw consent at any time and ensure that the procedure for withdrawing consent is just as simple as granting consent.

## **9. Privacy Notices**

- 9.1 Under the ‘fair and transparent’ requirements of the first data protection principle, the College is required to provide Data Subjects with a ‘privacy notice’ to let them know what it does with their Personal Data. Separate privacy notices have been published for learners and staff and are at Appendix 3 and 4.
- 9.2 Privacy notices are published on the College website and are therefore available to staff and learners from their first point of contact. Any processing of staff or learner data beyond the scope of the standard privacy notice, or processing of the personal information of any other individuals will mean that a separate privacy notice will need to be provided.

## **10. Data Sharing**

- 10.1 Certain conditions need to be met before Personal Data can be shared with a third party or before an external Data Processor is used to process data on behalf of the College. As a rule, Personal Data should not be passed on to third parties, particularly if it involves special categories of Personal Data but there are certain circumstances when it is permissible:
  - a) Any transfers of Personal Data must meet the data processing principles, in particular it must be lawful and fair to the Data Subjects concerned
  - b) It must meet one of the conditions of processing. Legitimate reasons for transferring data would include:
    - That it was a legal requirement.
    - It is necessary for the official core business of the College.
    - If no other conditions are met, then consent must be obtained from the Data Subject concerned and appropriate privacy notices provided.

- The College is satisfied that the third party will meet all the requirements of UK GDPR, particularly in terms of holding the information securely
- Where a third party is processing Personal Data on behalf of the College a written contract must be in place. A contract is also advisable when data is being shared for reasons other than data processing, so the College has assurances that UK GDPR requirements are being met. The College's UK GDPR compliant procurement standard Terms & Conditions must be agreed with all suppliers.

## **11. Subject Access Requests**

- 11.1 UK GDPR gives Data Subjects the right to access personal information held about them by the College. The purpose of a subject access request is to allow individuals to confirm the accuracy of Personal Data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information the College holds about them which includes copies of email correspondence referring to them or opinions expressed about them.
- 11.2 It should be noted that in most cases the College will no longer be able to charge for Subject Access Requests. HRUC will have 1 month from the receipt of the request to comply. The College will be able to refuse or charge a "reasonable fee" for requests that are manifestly unfounded, excessive or repetitive. If HRUC does refuse a request, it must tell the individual why and that he/she has the right to complain to the ICO or go to court. The policy and process covering Subject Access Requests is produced as a standalone policy.
- 11.3 The Freedom of Information Act 2000 (FOIA) enables greater public access to information processed by public bodies such as HRUC. However, Personal Data continues to be protected by the UK GDPR and is likely to be exempt from disclosure under the Freedom of Information Act (Section 40). However, this exemption does not apply to all personal data subject to a FOIA request, so advice from the DPO must be sought when dealing with a FOIA request involving Personal Data.

## **12. Data Retention**

- 12.1 Individual areas within the College are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on College guidance (see standalone Retention and Disposal of Data Policy). Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance.
- 12.2 Personal Data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed, it should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted. If data is fully anonymised, then there are no time limits on storage from a data protection point of view.
- 12.3 If College staff feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, they should contact the Data Protection Officer for guidance.

## **13. Data Protection (Privacy) by Design and Data Protection Impact Assessment**

- 13.1 Data protection by design and default is now a legal obligation for Personal Data. UK GDPR introduces a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (DPIA). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:
- a) Describe the collection and use of Personal Data
  - b) Assess its necessity and its proportionality in relation to the purposes
  - c) Assess the risks to the rights and freedoms of individuals
  - d) The measures to address the risks.
- 13.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The HRUC procedure for considering and processing a DPIA is at Annex A.
- 13.3 Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.
- 13.4 Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.
- 13.5 Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):
- a) Large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling where legal or similarly significant decisions are made.
  - b) Large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data
  - c) Systematic monitoring of public areas on a large scale e.g. CCTV cameras.
- 13.6 All DPIAs must be reviewed and approved by the Data Protection Officer.

## **14. Security**

- 14.1 The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.
- 14.2 All College users of Personal Data must ensure that all Personal Data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. Data Security should be undertaken in line with the College's Information Technology Security Policies and UK GDPR.

## **15. Personal Data Breach**



15.1 The College is responsible for ensuring appropriate and proportionate security for the Personal Data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The College makes every effort to avoid Personal Data breaches, however, in today's environment it is possible that a security breach could happen. Examples of Personal Data breaches include:

- a) Loss or theft of data or equipment
- b) Inappropriate access controls allowing unauthorised use
- c) Equipment failure
- d) Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- e) Human error
- f) Hacking attack

15.2 There are three main types of Personal Data breach which are as follows:

- a) Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a member of College staff is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong learner, or disclosing information over the phone to the wrong person
- b) Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key
- c) Integrity breach - where there is an unauthorised or accidental alteration of Personal Data.

15.3 If a data protection breach occurs the College is required in most circumstances to report this as soon as possible to the ICO, and not later than 72 hours after becoming aware of it. If you become aware of a data protection breach you must report it immediately. Details of how to report a breach and the information that will be required are in the Data Breach Notification policy and the Data Notification Procedure both of which are produced as standalone documents.

## **16. Transferring Personal Data to a Country Outside the EEA (European Economic Area)**

16.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be considered whenever the College appoints a supplier outside the EEA, or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

16.2 To ensure the College is compliant with Data Protection Laws College staff must not export Personal outside the EEA without the approval of the Data Protection Officer.

## **17. Appointing Contractors Who Access the College's Personal Data**

- 17.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.
- 17.2 One requirement of UK GDPR is that a Controller must only use Processors who meet the requirements of the UK GDPR and protect the rights of individuals. This means that data protection and due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.
- 17.3 Any contract where an organisation appoints a Processor must be in writing. The College is considered as having appointed a Processor where it engages someone to perform a service for the College and as part of it they may get access to the College's Personal Data. Where a Processor is appointed the College, as Controller remains responsible for what happens to the Personal Data.
- 17.4 UK GDPR requires the contract with a Processor to contain the following obligations as a minimum:
- a) To only act on the written instructions of the Controller.
  - b) To not export Personal Data without the Controller's instruction.
  - c) To ensure staff are subject to confidentiality obligations.
  - d) To take appropriate security measures.
  - e) To only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract.
  - f) To keep the Personal Data secure and assist the Controller to do so.
  - g) To assist with the notification of Data Breaches and Data Protection Impact Assessments.
  - h) To assist with subject access/individual's rights.
  - i) To delete/return all Personal Data as requested at the end of the contract
  - j) To submit to audits and provide information about the processing
  - k) To tell the Controller if any instruction is in breach of the UK GDPR or other EU or member state data protection law.
- 17.5 In addition, the contract should set out:
- a) The subject-matter and duration of the processing
  - b) The nature and purpose of the processing
  - c) The type of Personal Data and categories of individuals
  - d) The obligations and rights of the Controller.

## **18. Automated Decision Making and Profiling**

- 18.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to individuals:
- a) Automated Decision Making happens where the College makes a decision about an individual solely by automated means without any human involvement and the decision has legal or other significant effects,
  - b) Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

- c) Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If College staff therefore wish to carry out any Automated Decision Making or Profiling, they must inform the Data Protection Officer.

## **19. Direct Marketing**

- 19.1 The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.
- 19.2 Marketing consists of any advertising or marketing communication that is directed at particular individuals. When the College undertakes direct marketing, it will ensure that:
  - a) It provides adequate detail to individuals in its privacy notices, including, for example, whether profiling takes place.
  - b) It will operate on an 'opt-in' basis when seeking individuals' consent to continue to receive direct marketing communications.
- 19.3 The College will also comply with the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection.
- 19.4 Alternatively, the College may be able to market using a "soft opt in" if the following conditions are met:
  - a) Contact details have been obtained in the course of a sale (or negotiations for a sale). The College are marketing its own similar services.
  - b) The College gives the individual a simple opportunity to refuse to opt out of marketing, both when first collecting the details and in every message after that.

## **20. Children**

- 20.1 Under UK GDPR the age of consent is set at under 16. However, the UK legislation is set at under 13 and takes primacy. Although it is therefore unlikely the College will come into contact with a child's Personal Data it should be noted that the following restrictions apply to the processing of personal information relating to children:
  - a) Online services offered directly to children require parental consent
  - b) Any information provided to a child in relation to their rights as a Data Subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language
  - c) The use of child Data for marketing or for profiling requires specific protection.

## **21. Data Protection Training**

- 21.1 Relevant Data Protection Awareness training will be provided to staff to keep them better informed of relevant legislation and guidance regarding the processing of personal information. Data protection training will also promote awareness of the College's Data protection and information security policies, procedures and processes. Staff are strongly encouraged to complete this training during induction and subsequently on an annual basis.

## **22. Individual obligations**

22.1 You may have access to the personal data of others including members of staff, learners and other third parties who may come into contact with the College in the course of your employment or engagement. If so, the College expects you to help meet its data protection obligations to those individuals.

22.2 If you have access to personal data, you must:

- only access the personal data that you have authority to access, and only for authorised purposes;
- only allow other staff to access personal data if they have appropriate authorisation;
- only allow individuals who are not staff to access personal data if you have specific authority to do so from the DPO;
- keep personal data secure; and
- comply with all policies affecting your use of College personal data.

### **23. Consequences of failing to comply**

23.1 The College takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal data is being processed; and
- carries the risk of significant sanctions for the individual and the College; and
- may, in some circumstances, amount to a criminal offence by the individual.

23.2 Because of the importance of this policy any failure to comply with any requirement of it may lead to disciplinary action, which may result in termination of your relationship with the College.

### **24. College Point of Contact**

24.1 The nominated Data Protection Officer for the College is the Chief of Governance and Strategic Operations. All enquiries or requests for further information or guidance relating to Data protection should be emailed to [dpo@hruc.ac.uk](mailto:dpo@hruc.ac.uk).

## **PART 2: DATA SUBJECT RIGHTS POLICY**

### **1. DATA SUBJECT RIGHTS AND REQUESTS**

1.1 Data subjects have various rights in relation to their personal data. Dependant on the circumstances, data subjects have the right:

- a) to be informed about how, why and on what basis that data is processed (the College usually provides this information to data subjects via its Privacy Notice(s));
- b) to obtain confirmation that data is being processed and to obtain access to it and certain other information by making a subject access request;
- c) to have personal data corrected if it is inaccurate or incomplete (known as the right of rectification);
- d) to have personal data erased in certain circumstances (sometimes known as the right to be forgotten);
- e) to restrict the processing of personal their personal data in certain circumstances (e.g. if there is a complaint about accuracy);
- f) to object to the processing of their personal data in certain circumstances;

- g) to receive personal data that they have provided in a structured, commonly used and machine-readable format and to request that their personal data is transferred to another organisation (known as the right to data portability)

## **2. SUBJECT ACCESS REQUESTS**

- 2.1 Anybody has the right to ask the College for a copy of any personal data held about them, together with other information about how their data is used (known as supplementary information (see below). This legal right is called the right of access, often referred to as a subject access request or SAR.
- 2.2 There are some legal exemptions that mean that requesters may not always be entitled to a copy of all of their personal data that we hold.
- 2.3 As part of a subject access request, data subjects are entitled to the following supplementary information:
  - a) whether their personal data is being processed by the College;
  - b) the purposes of the processing;
  - c) the categories of personal data concerned;
  - d) the recipients or categories of recipient to whom their personal data have been or will be disclosed;
  - e) the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored;
  - f) the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing;
  - g) their right to lodge a complaint with the ICO;
  - h) where the personal data are not collected from the individual, any available information as to their source; and
  - i) details of the safeguards in place for any transfers of their data to locations outside the UK.
- 2.4 If you, as a member of staff, receive a SAR, you should immediately inform the DPO.
- 2.5 The College a duty to deal with SARs without delay and at the latest within 1 month of receipt (subject to the rights of the College to extend the time limit for response by a further 2 months, considering the complexity and number of the requests, in accordance with Article 12(3) of the UK GDPR).
- 2.6 Any individual may appoint another person to request access to their records. In such circumstances the College must have written evidence that the individual has authorised the person to make the request and the DPO must be confident of the identity of the individual making the request.
- 2.7 Where a person lacks capacity to understand their rights and the implications of making a subject access request (e.g. due to their age or some other reason) a third party, such as a parent or carer, can make a request on their behalf. The DPO must, however, be satisfied that:
  - a) the person lacks sufficient understanding of their own data rights; and
  - b) the request made on behalf of the person is made in the person's best interests.

- 2.8 Access to personal data may be restricted or refused in instances where an exemption under the DPA 2018 applies. For example, the relevant data is covered by legal advice privilege or data sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). The College must decide whether to apply any potential exemption (taking legal advice where appropriate), based on the circumstances of a particular request.
- 2.9 A subject access request may be made verbally or in writing. Where possible, the College prefers requests to be made in writing and using our prescribed subject access request form.
- 2.10 The College may ask the data subject for any further information reasonably required to locate the data.
- 2.11 All files must be reviewed and applicable exemptions under the UK GDPR and the DPA must be applied by the DPO. Any disclosure can only take place after the response is approved by the DPO. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the supplementary information the requestor is entitled to.
- 2.12 Where some of the data in a document cannot be disclosed a copy of the full document and the altered document should be retained, with the reason why the document was altered.

### **3. RIGHT TO RECTIFICATION**

- 3.1 Data subjects have the right to request the rectification of inaccurate or incomplete data verbally or in writing. Any request for rectification should be sent to the DPO immediately.
- 3.2 Where personal data is identified as inaccurate or incomplete, it shall be amended and the data subject notified of the same without undue delay and in any event within 1 month (unless this deadline is extended in accordance with the UK GDPR).
- 3.3 Where a request is refused, the request and reasons for refusal shall be documented and notice of refusal should be provided to the individual within 1 month of receipt of the request. The College will include in its response the reasons why the request has been refused and information about the individual's right to complain to the ICO and to bring a civil claim.

### **4. RIGHT TO ERASURE**

- 4.1 Individuals have a right, in certain circumstances, to have their personal data permanently erased. Individuals may exercise this right in writing or verbally.
- 4.2 The right to erasure is also known as the 'right to be forgotten' and arises in the following circumstances:
- a) where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
  - b) where consent is the legal basis for processing and that consent is withdrawn;
  - c) where legitimate interests is the legal basis for processing and the individual objects to the processing of their data, and there is no overriding legitimate interest to continue processing;
  - d) where the College is processing the personal data for direct marketing purposes and the individual objects to that processing;

- e) where personal data is being unlawfully processed;
  - f) where there is a legal obligation on the College to delete the personal data; or
  - g) where the College has processed the personal data to offer information society services to a child.
- 4.3 Any request for erasure should be sent to the DPO immediately. The request must be complied with within 1 month (unless this deadline is extended in accordance with the UK GDPR).
- 4.4 The DPO will determine the outcome of any request for erasure of personal data. Where a decision is made to erase the data, and this data has been passed to other controllers, and / or has been made public, the College will inform those organisations of the request unless this proves impossible or involves disproportionate effort.
- 4.5 Where a request is refused, the College will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

## **5. RIGHT TO RESTRICT PROCESSING**

- 5.1 In the following circumstances, individuals have the right to request the restriction or suppression of their personal data in writing or verbally:
- a) where the accuracy of personal data has been contested, during the period when the College is attempting to verify the accuracy of the data;
  - b) where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
  - c) where personal data would normally be deleted, but the individual has requested that their personal data be kept for the purpose of the establishment, exercise or defence of a legal claim;
  - d) where there has been an objection to the processing, pending the outcome of any decision.
  - e) Any request for restriction should be sent to the DPO immediately. The request must be complied with within 1 month (unless this deadline is extended in accordance with the UK GDPR).
- 5.2 The DPO will determine the outcome of any request for restriction of processing personal data. (As matter of good practice, the College will automatically restrict the processing whilst considering the accuracy or legitimate grounds for processing the personal data in question.)
- 5.3 Where processing has been restricted, such personal data shall (with the exception of storage) be processed only in the following circumstances:
- a) with the consent of the data subject;
  - b) where processing is necessary for the establishment, exercise or defence of legal claims;
  - c) for the protection of rights of another person (including a company); or
  - d) for reasons of important public interest.
- 5.4 If the College has disclosed the personal data in question to others, it will contact each recipient to inform them of the restriction, unless this proves impossible or involves disproportionate effort.

- 5.5 Once the College has determined the accuracy of the data, or whether the College's legitimate grounds override those of the data subject, the College may decide to lift the restriction. The College will inform the requestor before the restriction is lifted.
- 5.6 Where a request is refused, the College will inform the individual without undue delay and within 1 month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

## **6. RIGHT TO OBJECT**

- 6.1 Where personal data is being processed for direct marketing purposes, an individual has the right to object at any time to processing of their personal data for such purposes.
- 6.2 This right is absolute and where such an objection is made the College must stop processing personal data for this purpose.
- 6.3 An individual also has the right to object to the processing of their personal data on the legal basis of:
- a) a task carried out in the public interest;
  - b) the exercise of official authority vested in the College; or
  - c) the legitimate interests of the College or a third party.
- 6.4 Where such an objection is made, it must be sent to the DPO immediately. The DPO will assess whether the processing should cease or whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals concerned, or whether the data is required for the establishment, exercise or defence of legal proceedings.
- 6.5 The DPO is responsible for notifying the individual of the outcome of their assessment without undue delay and within 1 month of receipt of the objection (unless this deadline is extended in accordance with the UK GDPR). If the request is refused, the response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

## **7. RIGHT TO DATA PORTABILITY**

- 7.1 Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to require the College to transmit that personal data directly to another controller in certain circumstances.
- 7.2 This right only applies to data provided to the College directly by the data subject and:
- a) the processing is on the basis of consent or to perform a contract; and
  - b) the processing is carried out by automated means (i.e. on a computer).
- 7.3 If such a request for this is made, it should be forwarded to the DPO immediately and this will be reviewed and actioned as necessary.