UK GRADUATE
power through education

Data Protection Policy

Version 3.1

Updated on 01/02/2022
Review Date 31/01/2024
Responsible Person: Chief Executive and Principal – Shebul Ali

1. Statement of Intent

1.1 Individuals whose information is processed by UK Graduate (the college) can be assured that UK Graduate intends to fulfil all its Data Protection obligations. This policy document applies only to information covered by the Data Protection legislation, Data protection legislation means (i) the Data Protection Act 2018 and, for the periods when they are in force, (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) and any applicable national implementing laws as amended from time to time.

2. Introduction and Purpose

2.1 The college needs to keep certain information about its employees, students and other users to monitor performance, achievements, health and safety and other legal responsibilities. It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

3. Statutory Framework

3.1 The college must comply with the Data Protection principles, which are set out in the Data Protection Act (2018) (DPA) and the General Data Protection Regulations (GDPR).

In summary these state that personal data shall:

a. be processed lawfully, fairly and in a transparent manner in relation to individuals.

b. be 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.

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

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

e. be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals, and

f. be 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.

3.2 UK Graduate and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the college has developed this Data Protection Policy.

3.3 UK Graduate must also comply with Rehabilitation of Offenders Act 1974, Children Act 1989 and other legislation relating to Further and Higher Education delivery.

4. Related Policies and Procedures

a. Student Acceptable Use Of IT Resources Policy And Procedure

5. The Designated Data Controller

5.1 The college as a corporate body is the Data Controller under the Act, and the college Corporation is therefore ultimately responsible for implementation. However, the designated data controller will be responsible for:

a. Maintaining the college's registration with the Information Commissioner's Office.

b. Providing advice, guidance and direction on data protection issues within the college.

5.2 The college has a designated data protection officer who is the named person in the notification to the Information Commissioner. This is the Chief Executive Shebul Ali.

6. Extent of the Policy

6.1 The Data Protection Policy covers all computerised and manual data processing relating to identifiable living individuals. It not only includes information about individuals, but also options and intentions towards an individual. It therefore includes, for example, personnel records about staff, student records, and emails relating to identifiable individuals, curriculum team meeting minutes, student and staff references.

7. Status of the Policy

7.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the college from time to time. Any failures to follow the policy may therefore result in disciplinary proceedings.

7.2 Any member of staff or student, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data protection officer initially. If the matter is not resolved it should be raised as a formal grievance.

8. Rights to Access Information

8.1 Staff, students and other users of the college have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact the Human Resources (HR) (staff) or Student Services (students).

8.2 In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing to HR or Student Services.

8.3 The college will comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 28 days. Should the college not be able to produce the requested data within this time scale full information will be provided as to the reasons for this. The college may apply a reasonable fee when requests are deemed excessive or particularly repetitive but full information will be provided should this be the case.

8.4 Under GDPR regulations individuals have the right for removal of their consent to data being held. However, some data is required to be retained for audit and legal purposes; this data

will be securely removed following the retention period. In order to request removal of data, please contact HR (staff) or Student Services (students) who will be able to let you know which information can be removed and when. Individuals also have the right to data portability. Should they wish for their data to be transferred these requests should be made in writing to admin@ukgraduate.org.uk.

9. Consent

9.1 In many cases, the college can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the college processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974 and information about disabilities

9.2 Some jobs or courses will bring applicants into contact with children, including young people between the ages of 16 and 18 and vulnerable adults. The college has a duty under the Keeping Children Safe in Education and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The college also has a duty of care to all staff and students and must therefore make sure that employees and those who use the college facilities do not pose a threat or danger to others.

9.3 Therefore, all prospective staff and students will be asked to consent to their data being processed when an offer of employment or a course place is made. A refusal to sign such a form will result in the offer being withdrawn. This consent forms part of the Privacy Statement on the college websites and paper forms.

9.4 The Government and statutory organisations are exempt from the DPA and GDPR regulations, and on receiving a valid “legal exemption certificate” the college will release the requested information to the relevant authorities.

10. Data Sharing

10.1 As a student or staff member of the college it may be necessary on occasion to share your data with third parties including but not limited to Her Majesty’s Revenue and Customs (HMRC), Education and Skills Funding Agency (ESFA), Office for Students (OFS), Student Loan Company (SLC) and Local Authorities. You will be informed through privacy notices and consent forms that you have the right to withhold consent. However, the college may not be able to progress with your offer of employment/education without this. There are occasions where the college has a legal obligation to share information with authorities without consent from individuals. There is no right to references under current legislation; these may be provided by the college with explicit consent from the individual but will be limited to the data held within the relevant retention periods.

11. Special Categories of Personal Data

11.1 Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person’s fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual’s:

- Race
- Ethnic origin

- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

11.2 In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

11.3 The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing special categories of data that processing activity must cease.

12. Retention of Data

12.1 The college will keep some forms of information for longer than others in accordance with legal or statutory obligations.

12.2 Appendix 1 indicates the length of time that records will be retained.

13. Telephone Recording / CCTV

13.1 The college may record telephone conversations for the purpose of training and development and to protect staff and students.

13.2 The college telephone system has the capability to identify sources of calls both internally and externally to the college.

13.3 The college uses CCTV to help prevent crime and for the welfare, health and safety of employees, students and visitors. CCTV will be in operation throughout the college's premises and images securely stored for 30 calendar days, unless a criminal offense has occurred, then it will be handed to the police.

14. Roles and Responsibilities

14.1 All staff and students are responsible for:

a. Checking that any information that they provide to the college in connection with their employment or education is accurate and up to date.

b. Informing the college of any changes to or errors in information, which they have provided, i.e. changes of address. They must ensure that changes of address, etc are notified to the Human Resources (staff) and Student Services (students) Admissions (prospective students).

c. The college cannot be held responsible for any such errors unless the staff member or student has informed the college of them.

14.2 If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students' course work, opinions about ability, references to other academic institutions,

or details of personal circumstances), they must comply with the Staff Guidelines in Appendix 2.

14.3 IT staff will ensure the college is appropriately protected from external threats for the network and systems under their control.

15. Data Security

15.1 Data Protection Impact Assessments (DPIA)

a. The college will carry out data protection impact assessments for any new college product, process or procedure that will have an impact on the use of student or staff data. See Appendix 3 for format.

b. We always carry out a DPIA if we plan to:

i. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.

ii. Process special category data or criminal offence data on a large scale.

iii. Systematically monitor a publicly accessible place on a large scale.

iv. Use new technologies.

v. Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.

vi. Carry out profiling on a large scale.

vii. Process biometric or genetic data.

viii. Combine, compare or match data from multiple sources.

ix. Process personal data without providing a privacy notice directly to the individual.

x. Process personal data in a way which involves tracking individuals' online or offline location or behaviour.

xi. Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.

xii. Process personal data which could result in a risk of physical harm in the event of a security breach.

15.2 Staff Obligations

a. All staff are responsible for ensuring that:

i. Any personal data held is kept securely, for example in a locked room, locked filing cabinet or locked drawer.

ii. If it is computerised, it is password protected. All passwords shall be regularly changed.

iii. Data stored on disks is removed before disposal.

iv. Papers containing personal information are shredded before disposal or securely disposed of by other means.

v. Databases are closed and workstations securely locked when leaving the computer.

vi. Personal information is not disclosed either orally or in writing either accidentally or otherwise to any unauthorised third party.

vii. No personal details should be sent via email unless as part of an encrypted attachment with passwords sent via separate email.

viii. Staff should ensure that no personal data is transported on mobile devices including USB drives, USB drives should only be used to hold personal data with permission from line managers with relevant encryption software installed.

ix. Laptops and mobile devices used by staff travelling between campuses or for the purpose of working from home must be password protected. It is the responsibility of the staff member to maintain the security of equipment and data at all times. Personal data should not be stored locally on laptops and must be saved on the college network and accessed from there.

x. Any personal details that have to be scanned and shared must be done with consent of the person whose data is being scanned and securely removed from the scanning device and subsequent electronic storage following retention protocols.

xi. No personal details of any individuals should be printed or copied without prior consent from the individual and any copies should be securely disposed of following retention protocols.

xii. Any photographs or video taken of individuals must be stored securely with the explicit consent from the individuals for this storage and use.

xiii. Cloud storage should not be used for storage of any personal data including photographs and videos due to the inability to ensure data storage geographical location with the exception of approved providers, list of approved providers is available from Administration Team.

xiv. Training is kept up to date annually as provided by the college.

xv. That this policy is followed at all times.

b. Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

15.3 Data Breaches

a. Should a personal data breach be detected it will be immediately notified to the Data Protection Officer who will assess the severity of the breach, assessing the risk to individuals and the action to be taken and the breach recorded. The Data Protection Officer will notify the Information Commissioner's Office of all data breaches where a risk to individual's rights and freedoms has been identified.

b. Staff should immediately notify their line managers, Directors and Chief Executive (the Data Protection Officer). Alongside this, the breach information should be sent to admin@ukgraduate.org.uk flagged as urgent.

c. Students should immediately notify Student Services who will notify the Chief Executive and Chief Quality Assurer. Alongside this the breach information should be sent to admin@ukgraduate.org.uk flagged as urgent.

16. Monitoring, Review and Evaluation

16.1 The college will review this policy every two years or sooner in order to take account of new statutory regulations and recommendations for improvement.

17. Data Protection Audits

17.1 Audits of computerised and manual record systems should be conducted annually.

18. Communication

18.1 The policy is published on the college Intranet for members of staff. Its review will be communicated by sending an e-mail to all staff; included in the staff newsletter; at staff briefings and/or at professional development days to provide, when required, training to new employees. All new staff will be given a copy of this policy alongside other key college policies as part of their induction.

18.2 All students will be directed to read this policy and informed of this during enrolment and induction.

18.3 Under the requirements of the Freedom of Information Act 2000, the policy will be listed in the Publication Scheme and made available to the general public on request.

Appendix 1

Summary Guidelines for Archiving Data

Area	Description	Retention	Reason for Collection/Retention
Human Resources	Records documenting the successful appointment of members staff.	Termination of appointment + 6 years	HMRC Safer Recruitment
Human Resources	Records documenting staff name, dates and role	Termination of appointment + 10 years	Safer Recruitment
Human Resources	Records documenting the unsuccessful appointment of members staff.	6 months	Employment Tribunals
Human Resources	Sickness and health & safety records	Termination of appointment + 40 years	Potential Legal Cases
Human Resources	Details of DBS and any safeguarding concerns	Indefinitely	Safer Recruitment & Potential Legal Cases
Financial Resources	Records relating to financial services	Current financial year + 6 years	Audit
Financial Resources	Records relating to funding received that may be receiving European Social Fund (ESF) match funding	Current financial year + 12 years	ESF Audit
Student Records	Records relating to students funded as 16-18 year olds	Current financial year + 6 years	Audit
Student Records	Records relating to students funded as Adults that may be receiving ESF match funding	Current financial year + 12 years	ESF Audit
Student Enquiries	Data relating to enquiries for prior to application	Current financial year + 2 year	Potential follow up
Student Applications	Data relating to unsuccessful student applications	Current financial year + 1 year	Potential appeals
Examinations	Student results and achievements records	Current financial year + 10 years	Audit
Learning support	Details of learning support for students	Current financial year + 7 years	Audit
Photographs	Photos taken as part of marketing events or curriculum requirements	Stored until requested to remove by individuals	Marketing and branding
Estates	Documentation relating to lettings and hiring of college assets.	Current financial year + 1 year	Potential Legal Cases
Estates	Images and video captured via CCTV	30 days	Health and Safety
Estates	Records relating to health and safety including accident logs	Current financial year + 40 years	Health and Safety legislation
Sports Centre	Membership records	Current financial year + 6 years	Audit

Ownership and Management of Archives
This includes keeping an up to date list of box numbers and disposal dates within the department, preferably by a document stored on the network drive, and also arranging for boxes to destroy soon after the disposal date – at least on an annual basis.

Storage and Labelling
Boxes should be clearly labelled with:

- Contents (and whether contents are confidential)
- Unique Box Number
- Disposal date

Appendix 2

Data Protection Act 2018

Staff Guidelines

- Members of staff will process personal data on a regular basis. The College will ensure that staff and students give their consent to processing and are notified of the categories of processing, as required by the Act and GDPR via privacy notices.

- Information about an individual's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive and can only be collected and processed with their explicit consent as this is not covered by legal obligations.

- Members of staff have a duty to make sure that they comply with the data protection and GDPR principles, which are set out in the College Data Protection Policy. In particular, staff must ensure that records are:

  - Accurate
  - Up to date
  - Fair
  - Used only for the purpose it was collected for
  - Kept and disposed of safely and in accordance with the College policy

- Individual members of staff are responsible for ensuring that all data they are holding is kept securely and securely removed following the retention guidelines and Data Protection Policy.

- Members of staff must not disclose personal data, unless for normal academic, administrative or pastoral purposes, without authorisation or agreement from the data controller, or in line with HR and the College policy.

- Before processing any personal data, all staff should consider the checklist as set out below.

- The HR, Finance and Administration offices are the only departments that should contain all information relating to employees' personal details. Locally stored information within Curriculum areas and departments must be used solely for purposes of communication and collection of any other type of personal data is prohibited.

UK GRADUATE
power through education

Staff Checklist for Recording Data

Do you really need to record the information?	
Is the information 'standard' or is it 'sensitive'? (Information about an individual's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive information)	
If it is sensitive, do you have the data subject's explicit consent?	
Has the individual or data subject been told why and how this data will be processed?	
Are you authorised to collect/store/process the data?	
If yes, have you checked with the data subject that the data is accurate?	
Are you sure that the data is secure?	
If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?	
Have you notified the Designated Data Protection Officer that you intend to hold the data?	
How long do you need to keep the data for, if longer than the retention period as per the Data Protection Policy the designated Data Protection Officer must be notified.	

UK GRADUATE
power through education

Appendix 3 Privacy Impact Assessment Template (PIA)

Step one: Identify the need for a PIA Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).
Step two: Describe the information flows You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks Identify the key privacy risks and the associated compliance and corporate risks. Larger scale PIA's might record this on a more formal register.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

UK GRADUATE
power through education

Step four: Identify privacy solutions
Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes
Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan
Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	**Date for completion of action**	**Responsibility for action**

Contact point for future privacy concerns