UCG Data Protection Policy

Summary

This policy describes how the College protects personal data.

Policy Owner:	Assistant Principal IT
Preparation Date:	April 2018
Approval/ Review Body:	Governing Body
Review Date:	September 2018

Introduction

1. United Colleges Group controls and processes the personal data of staff, students and to a lesser extent visitors, contractors and suppliers. This policy is designed to ensure UCG complies with the law. The UK Data Protection Act of 1998 (DPA) is being replaced by the General Data Protection Regulation (GDPR) on 25th May 2018. The new regulation carries a legal obligation to protect the fundamental rights of individuals when their personal data is outside their control and could lead to their privacy being compromised. A new data protection bill is currently passing through parliament this will supplement GDPR. The new bill will update the rights of individuals to make them easier to exercise and to ensure they continue to be relevant in the face of rapidly changing technology.

2. Personal data is defined as any information relating to an identified or identifiable natural living person. That is identifiable directly or indirectly for example a CCTV image, an email address that identifies the individual, an ID number or name and DOB.

3. Under the legislation The College is defined as a public authority and processes student data under the lawful basis of public task, legal obligation, and vital interest, for alumni data legitimate interest. Full details are in the privacy notice legal bases for processing data. Staff data is processed under the lawful bases of legal obligation and legitimate interest.

Status of the Policy

4. This policy does not form part of the formal contract of employment, but it is a condition of employment that staff will abide by the rules and policies made by the College from time to time. Any failure to follow the policy may result in disciplinary action.

5. Any member of staff or any 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.

Data Protection Principles and responsibilities

6. Information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles set out in the General Data Protection Regulation by ensuring that data protection principles are adhered to. Article 5 of the GDPR requires that personal data shall be:

    a. **Transparent:** processed lawfully, fairly and in a transparent manner in relation to individuals;

    b. **Limited:** 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. **Minimal:** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

    d. **Accurate:** 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. **Have clear retention periods:** 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. **Have integrity and be confidential:** 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.

7. The College is both a data controller and a data processor and is therefore responsible for compliance with the data protection principals. The College must be able to demonstrate that it is compliant with article 30 of the GDPR by maintaining records of all data processed (data flows and data sets), the purpose of processing, who data is shared with and how long data is retained.

8. Senior managers with responsibility for data; (HR, MIS, IT, Security, Supported Learning Business Development, Finance, Student Finance and Supported Learning) must ensure that records of data processed are accurate, annually updated, maintained and that records are deleted in accordance with the retention policy.

9. The data protection officer will conduct annual audits of data processing and decide whether or not a data impact assessment is required.

10. United Colleges Group and all staff or others who process or use any personal information must ensure that they follow these principles at all times.

The rights of data subjects

11. All data subjects (staff, students, visitors and other whose personal data is held by the College) have the following rights:

12. **The right to be informed.** Individuals have the right to be informed about the collection and use of their personal data, this is a key transparency right under GDPR. Data subjects must be provided with information including; the College's purpose for processing their personal data, retention periods for that personal data, and who it will be shared with. This is called 'privacy information' and must be provided to individuals at the time the College collects their personal data from them

13. Senior managers listed in paragraph 7 must ensure privacy information is concise, transparent, intelligible, easily accessible, and it must use clear and plain language. Privacy information must be regularly reviewed, and where necessary, updated. Any new uses of an individual's personal data must be brought to their attention before you start the processing.

14. **The right of access.** Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed, access to their personal data and other supplementary information, (this is normally provided in the privacy statement). Such subject access requests (SAR) must be sent to the Data Protection Officer and data provided within 1 calendar month. The College cannot charge for this service except in rare circumstances refer to GDPR guidelines https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

15. An individual can make a request for rectification, erasure, and restricted processing verbally or in writing. The College has one calendar month to respond to a request. All requests must be recorded and a response to the individual given. Senior managers (paragraph 7) must ensure they have a system for recording requests and responses to these rights (paragraphs 15 to 17 below). Managers must ensure that staff are briefed on how to handle such requests

16. **The right to rectification.** Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. There are situations where it may not be possible to rectify data for guidance see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

17. **The right to erasure**. Individuals have the right for personal data erased, also known as 'the right to be forgotten'. The right to erasure does not apply if processing is necessary for example: to comply with a legal obligation. Managers must check the ICO website before refusing to erase data. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

18. **The right to restrict processing.** Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right, when processing is restricted, the College is permitted to store the personal data, but not use it. Managers must check the ICO website if refusing the right to rectification. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

19. There are 3 further rights; the right to data portability, the right to object and rights in relation to automated decision making and profiling. Any requests from individuals invoking these rights must be referred to the data protection officer.

Responsibilities of Staff and Students

20. All members of staff and students are responsible for:

    a. Checking that any information that they provide to the College in connection with their employment or enrolment is accurate and up to date.
    b. Informing the College of any changes to information, which they have provided, e.g. change of address.

Data Security Staff responsibilities

21. All members of staff are responsible for ensuring that:

    a. Any personal data which they hold is kept securely.
    b. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

22. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

23. Staff must report data breaches to the DPO without delay.

24. Other than for emergencies where next of kin data can be used, parents of students aged over 18 must not be contacted unless we have the permission of the young person recorded centrally and the permission of the parent also recorded centrally, unless there are issues around the student's competency to understand key matters and the College needs to consult a parent, guardian or social worker

25. Personal information should be kept in central college systems such as the MIS, HR, ILP & tracking, finance and supported learning systems. Staff should not keep personal data in their own spreadsheets, databases or other application software. If the data needs to be printed great care must be taken to ensure only those authorised to see such data are able to. Where possible such data should be anonymised.

26. Where central systems do not support the processes needed this must be recorded as outlined in paragraph 6. Such data must not be shared via email unless encrypted using the College's encryption software currently Egress. Staff are encouraged to share data via Office 365 which is secure.

27. All college owned mobile devices and any USBs used in the college will be encrypted, this encryption must not be removed. USBs must not be used to store personal data.

28. Staff using their own or college mobile devices to access college data and systems will have an MDM application installed on their device. All data must be accessed via this application. On leaving the college this data will be erased by IT. All such devices must be password protected (see the data security policy for guidelines on strong passwords).

29. Great care must be taken when transporting or accessing personal data outside of college premises whether this is held on paper on mobile devices. Personal data must

not be left in public places or accessed in places where you could be overlooked. Password controlled screen savers must be used.

30. Paper records must be kept in locked filing cabinets or drawers. In some cases such as HR and supported learning managers of those areas should regularly review the need to restrict entry.

31. Teachers who hold personal information such as course work and exam results must ensure these are kept securely in locked filing cabinets or desk drawers and confidentiality is maintained.

Organisations and others to which to the College may Provide Data

32. The College may provide data relating to staff and students to organisations, including but not limited to, Government Departments including the Department for Education, HMRC, the disclosure and barring service, the Funding Councils (including the Education and Skills Funding Agency, and the Higher Education Funding Council for England), Local Education Authorities, Student Loans Company, Awarding Organisations, Sub Contractors, Universities, Police, auditors, pension providers, First Care and, for those receiving benefits, the Department for Work and Pensions. It may also be the case that personal information is provided to such organisations through agencies acting on their behalf.

33. Where data is shared this must be clearly stated in the privacy information given to the data subject.

34. Where data is shared with a third party organisation the College will ensure a signed data sharing contract is in place that ensures data processed complies with GDPR

Processing Sensitive Information (special category data)

35. Sometimes it is necessary to process information about a person's health, criminal convictions, race, sexual orientation, gender re-assignment, religion, marriage / civil partnership, pregnancy / maternity, gender, disability and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy or to provide statistics/equalities monitoring data to government agencies. This conforms to the conditions for processing special category data in article 9 of the GDPR specifically conditions b, h and j. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

36. The lawful bases for processing such data is public task, legal obligation and vital interest to ensure the college is a safe place to study and to meet our obligation to provide statistics/equalities monitoring data to government agencies.

37. Offers of employment or course places may be withdrawn if an individual refuses to provide this data. More information about this is available from the Director of Human Resources (employment offers) or Assistant Principal Information and Planning (course place offers).

CCTV

38. The College operates a number of CCTV cameras in order to assist with the security of the College and protect property and individuals. If any individual has any queries regarding the operation of the CCTV system, they should contact the data protection officer. The images are held in secure conditions for 28 days, and on the 29th day they are erased. If anyone wishes to access any personal data about themselves on the CCTV system within 21 days of the occurrence, they should contact the data protection officer with as much information as possible to enable the data to be located (including, if possible, details of the location of the camera, date and time).

The role of the Data Protection Officer

39. The UCG Corporation is ultimately responsible for implementation of the GDPR and the Data Protection Bill. As a public authority the corporation must appoint a data protection officer (DPO) who shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks listed in the GDPR. The DPO should be independent and not be subject to conflicts of interest and report to the highest management level.

40. The DPO is the first point of contact for any enquiries relating to Data Protection issues. Contact details for the DPO will be published in all privacy notices.

41. The DPO is responsible for the following:

    a Providing information and advice to data controllers, data processors and data subjects
    b Monitoring compliance with the GDPR, other data protection laws, and our data protection policies
    c annual audits and impact assessments
    d Cooperating with the ICO
    e Dealing with subject access requests within 1 month of receipt
    f Reporting data breaches to the ICO within 72 hours

42. The following managers have specific responsibilities for data control and processing and will report to the DPO on matters related to data protection

Post	**Area of Responsibility**
Group Executive Director of Human Resources	For personal information about College staff
Assistant Principal IT	For information related to the College registration under the Data Protection Act and the security of IT facilities
Estates Managers	CCTV and Security
Head of Marketing	For external communications that rely on personal data and Alumni personal records
Director of Business Development	For personal data about students enrolled as Apprentices/ students on commercial courses and data shared with delivery partners

Director of Community Studies/Head of supported Learning	For personal data about college students relating to learning difficulties and disabilities
Head of Student Services/Group Executive Director of Finance	For personal data about students who have applied for bursaries/hardship/student loans and are entitled to free school meals

Retention of Data

43. Retention periods will be shown in privacy statements and recorded in 'article 30' spreadsheet

44. The named managers in paragraph 30 are responsible for ensuring retention periods are adhered to

45. The DPO will carry out audits of compliance

Disposal of Data

46. When personal data is no longer required, or has passed its retention date, paper records must be shredded. If there is a significant amount of material which cannot be dealt with by normal shredding machines, this should be disposed of using a secure waste disposal sack.

47. Computerised records must be permanently deleted, with particular care taken that 'hidden' data cannot be recovered. The IT Helpdesk can advise on permanent deletion of computerised records.

Conclusion

48. Compliance with the GDPR and data protection law is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated DPO

Useful Links and Reference Sites

- The Information Commissioner responsible for enforcement of the Data Protection Act - http://www.ico.gov.uk/.
- For advice and guidance on interpretation of the Data Protection Act in FE and HE Institutions - JISC Legal http://www.jisclegal.ac.uk/.
- For advice and guidance on retention periods for Further Education Institutions – JISC InfoNet Retention Schedules for FE http://bcs.jiscinfonet.ac.uk/fe/.