UNIVERSITY COLLEGE
OF ESTATE MANAGEMENT

UCEM Data Protection Policy

Version:	13.00
Status:	Final
Owner:	Data Protection Officer
Date:	2024-12-04

Approval History

Version	Date	Name
3	12/09/2017	Senior Leadership Team
4	18/10/2017	GDPR Working Group
5	09/11/2017	GDPR Working Group
6	06/12/2017	Board of Trustees
7	17/09/2018	GDPR Working Group
8	13/12/2018	Board of Trustees
9	26/03/2020	Board of Trustees
10	25/03/2021	Board of Trustees
11	31/03/2022	Board of Trustees
12	18/04/2024	Board of Trustees
13	04/12/2024	Board of Trustees

Document History

Version	Date	Reason	Person
0.01	31/07/2017		
1.01	04/08/2017	Guidance moved to appendices	Liz Howlett
2.01	12/09/2017	Highlighting questions and updating	Liz Howlett
3.01	10/10/2017	Incorporating comments from consultation with GDPR Working Group	Liz Howlett
4.01	09/11/2017	Comments from GDPR Working Group meeting	Liz Howlett
5.01	06/12/2017	Board of Trustees	Liz Howlett
6.01	31/07/2018	GDPR and DPA 2018 updating	Liz Howlett
7.01	13/12/2018	Annual review	Liz Howlett
8.01	07/02/2020	Annual review	Lucy Roper
9.01	15/02/2021	Annual review	Lucy Roper
10.01	17/02/2022	Alignment with internal structure changes; collection notices replaced with links; general drafting changes	Andy Youell

11.01	22/03/2024	Updated in line with Data Audit findings	Andy Youell
12.01	01/11/2024	Annual Review – updated to include sections relating to personal data breaches, data retention and destruction, and management of the policy itself.	Data Protection Officer

Table of Contents

1. Introduction

This Policy has been prepared with due regard to the data protection laws applicable to UCEM and our Personal Data Processing activities. These Data Protection Laws include the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018").

UCEM collects, stores and processes personal data in order to run the business and to meet statutory, regulatory and audit requirements. UCEM is registered with the Information Commissioners Office (ICO) as a Data Controller.

This policy applies to all UCEM employees, workers and contractors ("you", "your"). Your compliance with this policy is mandatory. Any breach of this policy and our other data protection policies/procedures may result in disciplinary action, up to and including termination for serious offences. This policy applies across all territories and jurisdictions in which UCEM operates.

Throughout this policy references to students includes students studying as a part of an apprenticeship and students that are studying through the Online Academy.

This policy has been approved by the Data and Systems Governance Group and the UCEM Board of Trustees. It is reviewed annually.

The Board delegates authority to the Data and Systems Governance Group to update the policy, if required, to reflect guidance from the ICO.

Any changes to this data protection policy will be published on the UCEM website and you will be notified of changes by other communication channels if it is appropriate to do so.

2. Your Rights

You have the right to ask UCEM for a copy of your personal data. This is known as a data subject access request. You can submit a request via our Data Subject Rights Request form, available here.

You also have the right to:

- object to processing that is causing you, or is likely to cause you, damage or distress
- object to communications or direct marketing
- request a correction to your personal data
- request the erasure of your personal data
- lodge a complaint with the Information Commissioner's Office.

UCEM will retain student data indefinitely or until a student requests us to do otherwise. Where students exercise their right to erasure, UCEM will continue to maintain a core set of personal data (name, subject(s), record of learning and achievement and award details, unique UCEM identification number and date of birth) in order to ensure that the record of academic achievements is maintained.

UCEM may also need to retain some financial records about data subjects for statutory purposes.

UCEM will apply the public interest test when considering any request to delete personal data.

3. Definitions

3.1 Personal Data

Personal data means data which relates to a living individual who can be identified –

(a) from that data, or

(b) from that data and other information, which is in the possession of, or is likely to come into the possession of, the Data Controller.

This includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual. Personal data also includes personal identifiers that are used in computer systems.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be considered personal data.

3.2 Special categories of personal data

The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

The processing of personal data relating to criminal offences under the UK GDPR may only be carried out under the control of an official authority.

Special category data includes personal data revealing or concerning the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.

Personal data that has been pseudonymised[1] can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The categories of data are broadly drawn so that, for example, information that someone has a broken leg is classed as a special category of personal data, even though such information

[1] Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information.

is relatively matter of fact and obvious to anyone seeing the individual concerned. Clearly, details about an individual's mental health, for example, are generally more sensitive than whether they have a broken leg. UCEM will record any agreement to include special categories of data in records of conversations with students.

3.3 Data Protection Officer

The responsibility of the Data Protection Officer (DPO) is as follows:

- To inform and advise the organisation and its staff about their obligations to comply with the UK GDPR and DPA 2018 and other relevant laws.
- To monitor compliance with the DPA 2018 and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (staff, students etc.)

UCEM ensures that the DPO:

- Reports to the Board of Trustees
- Operates independently and cannot be dismissed, or penalised, for performing their task.
- Has adequate resources to enable them to meet the obligations under the DPA 2018

3.4 Consent

Consent under the DPA 2018 must be freely given, specific, informed and an unambiguous indication of an individual's wishes. There must be some form of clear affirmative action – a positive opt-in. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and there must be a simple way for people to withdraw consent.

4. Data Protection Principles

The data controller (UCEM) shall be responsible for, and able to demonstrate compliance with, the following principles:

4.1 Data must be processed lawfully, fairly and in a transparent manner

UCEM must:

- have legitimate grounds for collecting and using personal data;
- not use the data in ways that have unjustified adverse effects on the data subjects;
- be transparent about how data will be used and give data subjects the appropriate privacy notices when collecting their personal data;
- handle the personal data of both students, staff and contractors only in ways they would reasonably expect; and
- ensure that nothing unlawful is done with the data.

The lawful basis for the processing of data by UCEM is that processing

- is necessary for the performance of a contract with the data subject or to take steps to enter into a contract, and/or
- is necessary for compliance with the law, and/or
- has been carried out with the consent of the data subject.

UCEM will rely on the legitimate interests ground where the nature of the business requires that personal data be shared to carry out business functions such as client management or maintenance of software. UCEM will rely on public task where processing is necessary for the performance of a task carried out in the public interest.

There are specific areas where UCEM will process special categories of personal data. These are where processing is necessary for:

- the purposes of preventative or occupational medicine, for assessing the working capacity of a student or member of staff, medical diagnosis, the provision of health or social care or a contract with a health professional or a non-medical help supplier;
- archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes;
- recruiting and onboarding new staff;
- administering sickness absence reporting and sickness payment;
- administering employment benefits;
- managing health and medical matters during employment which may involve third party organisations, such as counsellors, advisors, GPs, Occupational Health, and other medical specialists and professionals.

4.2 Data can only be collected for specific, explicit, legitimate purposes

Data must not be further processed in a manner that is incompatible with those purposes, but 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.

UCEM supplies statistical data to the Higher Education Statistics Agency (HESA), Office for Students (OfS), The Education and Skills Funding Agency (ESFA) and to other statutory bodies (i.e. Ofsted) for the purposes of monitoring outcomes.

Please see Appendix 1 for links to relevant third-party collection notices.

4.3 Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

UCEM must ensure that the personal data held is sufficient but that no more is held than needed. UCEM will not hold information that will never be needed but UCEM may hold information for a foreseeable event that never occurs.

4.4 Data must be accurate and, where necessary, kept up to date.

Every reasonable step will 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

4.5 Data must 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 DPA 2018 in order to safeguard the rights and freedoms of individuals

4.6 Data must be processed in a manner that ensures appropriate security of personal data.

This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. Information Security

Security is a critical part of keeping information confidential. UCEM takes necessary and appropriate steps to ensure that all information is held securely both physically and electronically.

6. Data Protection by Design and Default

UCEM shall ensure that the risks to rights and freedoms of Data Subjects associated with processing are key considerations when:

a) Designing, implementing and during the life of business practices and processes that involve the processing of personal data (“processing activities”); and
b) Developing, designing, selecting, procuring, and using applications, services, products and other IT systems and technologies for collecting, holding, sharing, accessing, and otherwise processing personal data (“processing systems”).

This risk-led approach to processing activities and processing systems shall apply throughout the full lifecycle of the processing, from initial planning and setting of specifications, during use of processing systems, through to disposal of the personal data. It shall take into account both the likelihood and the severity of the potential harm to the rights and freedoms of Data Subjects.

Where the risk to rights and freedoms of Data Subjects is likely to be high, or where otherwise required by law or the relevant supervisory authority, a DPIA shall be performed in accordance with our DPIA procedure.

Safeguards and preventive measures shall be implemented into processing activities and processing systems from the outset and throughout the processing lifecycle, to mitigate the risks to data subjects and protect their rights. These safeguards and measures shall be proportionate to the risks and include organisational (e.g. policy, awareness, governance, and assurance) as well as technical measures (e.g. pseudonymisation). The objectives of such safeguards and measures shall include:

a) data minimisation
b) limiting the extent of the processing, storage, and access to what is strictly necessary
c) ensuring transparency for data subjects regarding the processing activities; and
d) ensuring the security of the personal data.

7. Data Sharing

There are two types of data sharing: systematic and exceptional

‘Systematic’ means a routine sharing of data or pooling of data.

‘Exceptional’ is one-off sharing (which might have to happen in an emergency)

When deciding whether to share data UCEM will consider the following:

- **What is the sharing meant to achieve**? We will have a clear objective or set of objectives. Being clear about this allows us to work out what data we need to share and who with. We will document this.
- **What information needs to be shared**? We won’t share all the personal data we hold about someone if only certain data items are needed to achieve our objectives.
- **Who requires access to the shared personal data**? We employ ‘need to know’ principles, meaning that other organisations should only have access to your data if they need it, and that only relevant staff within those organisations should have access to the data. This will also address any necessary restrictions on onward sharing of data with third parties.

- **When should it be shared**? Is this an on-going, routine process or should it only take place in response to particular events?
- **How should it be shared**? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
- **How can we check the sharing is achieving its objectives**? We will judge whether it is still appropriate and confirm that the safeguards still match the risks.
- **What risk does the data sharing pose**? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in us?
- **Could the objective be achieved without sharing the data or by anonymising it**?
- **Do we need to update our notification**?
- **Will any of the data be transferred outside of the European Economic Area (EEA)**?

7.1 Routine data sharing

Data will be shared routinely with government departments and other bodies involved in the funding and regulation of higher education. Depending on the particular arrangements for different students, this includes:

- the Education and Skills Funding Agency (ESFA)
- the Higher Education Statistics Agency (HESA) – more information at 7.3
- the Office for Students (OfS)
- the Student Loans Company (SLC)
- the Universities and Colleges Admissions Service (UCAS)

When students register with UCEM, they consent to this sharing of data.

Where data is shared routinely with other organisations a data sharing agreement will be in place.

7.1.1 Data sharing agreements

These will, at least, document the following issues:

- the purpose, or purposes, of the sharing;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- the data to be shared;
- data quality – accuracy, relevance, usability etc;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and

- sanctions for failure to comply with the agreement or breaches by individual staff.

7.1.2 Points we will consider before sharing:

Is the format of the data being shared compatible?

The IT team is consulted about the secure transfer of data and, if a data sharing agreement is required, the IT team are also consulted to ensure all IT requirements are acceptable and can be delivered. The format of the data being shared must be compatible with the systems used by all those sharing. We will check that information is held in the same way and that it is accurate. If we need to share data urgently, we will test how well the systems used for sharing the data work when it is not urgent.

Is the information we are sharing accurate?

We will agree how any incorrect data will be corrected by all parties

Agree common retention and destruction arrangements for the data sent and received

Staff in the area affected will be sufficiently trained to know when to share data and in what circumstances

7.2 Exceptional data sharing

UCEM complies with the Social Care Institute for Excellence guidelines on sharing information including compliance with the Prevent duty under the Counterterrorism and Security Act 2015. Information will be shared with the right people at the right time to:

- Prevent death or serious harm
- Coordinate effective and efficient responses
- Enable early interventions to prevent the escalation of risk
- Prevent abuse and harm that may increase the need for care and support
- Maintain and improve good practice in safeguarding students
- Reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse
- Identify low-level concerns that may reveal people at risk of abuse
- Help people to access the right kind of support to reduce risk and promote wellbeing
- Help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour
- Reduce organisational risk and protect reputation

7.3 The Higher Education Statistics Agency (HESA)

HESA and HEAT may share your data as detailed in their own privacy notices, which are accessible at the links provided in Appendix 1.

Student data will be stored on a scored database (the Higher Education Access Tracker – HEAT) and used to administer participation in success and progression activities and projects. For evaluation and monitoring purposes only, this data may also be shared with UCEM's Regulatory Compliance team to help run and evaluate the effectiveness of any activity.

8. Closed Circuit Television

Closed circuit television (CCTV) is a private television system involving video cameras that capture images for security, surveillance, law enforcement and general-purpose monitoring applications. Unlike public broadcast TV, it is a closed system intended for private use.

UCEM collects CCTV images, some of which will fall within the definition of Personal Data. These images are captured in order to provide a safe and secure environment for all staff and visitors at all UCEM sites. These images may be used to identify, apprehend and prosecute offenders and to identify actions where disciplinary action might be needed.

CCTV images are stored in a way that maintains the integrity of the information. They are kept securely, and access is restricted to authorised personnel. CCTV images will be viewed in a restricted area.

The retention period for CCTV images is informed by the purpose for which the information is collected.

9. Social media

UCEM has a corporate social media presence, the purpose of this is to inform and engage with stakeholders. UCEM corporate social media accounts are monitored at regular intervals and only these corporately owned and managed social media channels will be reviewed as part of any Data Subject Access Request.

Views expressed by UCEM staff or contractors on personal social media accounts should not be interpreted as being the views of UCEM. Personal social media accounts are not managed, monitored or held by UCEM. This could also represent an infringement of individuals privacy rights to disclose such information. As such these accounts will not be part of any review of information held by UCEM when it receives an DSAR.

10. Cookies

A cookie is a piece of information in the form of a very small text file that is placed on an internet user's computer. It is generated by a web server. The information the cookie contains is set by the server and can be used by that server whenever the user visits the site. It is like an ID card telling the website the user has returned. Cookies make the interaction between users and websites faster and easier. They save time and make browsing more efficient. If you use the internet to carry out certain transactions with UCEM, your computer will store these cookies.

Cookies cannot read your computer's memory or storage and they cannot make any information available to third parties. They are used so that our systems can easily recognise you when you return to our websites and, as a result, enable us to provide you with a better service. We also track user traffic patterns in order to determine the effectiveness of our website. We do not release this information to third parties. If you prefer not to receive cookies while browsing our website, you can set your browser to refuse them. However, if you are a registered student with UCEM you will need to allow "per-session" cookies in order to access password-protected sites.

The use of your personal information this way is necessary for the legitimate interests of UCEM in operating and improving its website, analysing the use and ensuring the security of the website. Our website collects very little personal information and we use it in ways that are compatible with your individual rights and freedoms. Where you enter your personal

information into an online form on our website for any specified purpose, you will be told about the use we will make of that information.

11. Data Breach Notifications

All Personal Data breaches must be reported immediately to the DPO and must be added to the register of Personal Data breaches.

Where UCEM is a Data Processor, and 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 Controller must be notified immediately with further information about the breach provided as soon as information becomes available.

Where UCEM is the Data Controller, unless a Personal Data breach occurs which is unlikely 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 relevant supervisory authority must be notified of the breach without delay, and in any event, within 72 hours after having become aware of it, if this is feasible. If the notification is not made within 72 hours, it should be made as soon as possible, together with reasons for the delay. The Information Commissioner's Office (ICO) is the supervisory authority in the UK.

In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of Data Subjects, all affected Data Subjects are to be informed of the breach directly and without undue delay.

Irrespective of whether UCEM is a Data Processor or a Data Controller, all data breach notifications must be handled strictly in accordance with the UCEM Personal Data Breach Procedure and be added to the UCEM Personal Data Breach Register.

12. Data Retention & Destruction

Where UCEM is a Data Processor, we may only retain Personal Data for the duration of the data processing agreement. Upon termination of the data processing agreement, we must, at the choice of the controller, delete or return all the Personal Data to the Data Controller and delete all existing copies unless otherwise required to store a copy by UK and/or EU member state law.

Where UCEM is the Data Controller, we may only retain Personal Data for as long as is reasonably required and in any event, only for as long as set out in the UCEM Personal Data Retention Policy.

Once Personal Data records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used.

13. Contact details

If you have any queries or concerns about the handling of your personal data, please contact the Data Protection Officer at: dataprotection@ucem.ac.uk

If you remain dissatisfied with the handling of your request or complaint, you have a right to appeal to the Information Commissioner. There is no charge for making an appeal. Contact details are:

The Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 01625 545745 or 0303 123 1113 (local rate)

14. Implementation & Policy Management

This policy shall be deemed effective as of 1st November 2024. No part of this policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This policy will be reviewed by the Data Protection Officer annually.

Appendix 1: Collection notices

The Higher Education Statistics Agency publishes collection notices for the HESA student and staff collections at https://www.hesa.ac.uk/about/regulation/data-protection/notices

The Education and Skills Funding Agency publishes a Privacy Notice at https://www.gov.uk/government/publications/esfa-privacy-notice

The Student Loans Company publishes a Privacy Notice at https://www.gov.uk/government/publications/student-loans-company-privacy-notice

The Universities and Colleges Admissions Service (UCAS) publishes a privacy policy at https://www.ucas.com/about-us/policies/privacy-policies-and-declarations/ucas-privacy-policy