UNIVERSITY COLLEGE OF ESTATE MANAGEMENT

UCEM Data Protection Policy

Version:	12.00
Status:	Final
Author:	Andy Youell
Date:	April 2024

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

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

Table of Contents

1. Introduction

The Data Protection Act 2018 (DPA2018) protects the rights of individuals to have their personal data collected and stored securely and used only for legitimate and lawful purposes for which their consent has been sought. DPA2018 is based on the General Data Protection Regulation 2016 (GDPR) which is a European Union regulation. GDPR sets out the rights of individuals and the accountability of organisations on issues of data processing. Following Brexit, GDPR has been retained and continues to apply in the UK, known as the UK GDPR.

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 sets out how the University College of Estate Management (UCEM) and UCEM Asia Ltd complies with DPA2018. 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 Senior Leadership Team and the UCEM Board of Trustees. It is reviewed annually.

The Board delegates authority to the Data Protection Officer 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 and details of this process are set out in Appendix One.

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 at https://ico.org.uk/concerns/
- seek compensation for damages caused by a breach of the UK GDPR.
- request restriction of processing
- request the right to data portability

UCEM will retain student data in accordance with the institution's retention policy and schedule. 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.

To exercise any of the rights above, please contact the Data Protection Officer at dataprotection@ucem.ac.uk .

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 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

The Data Protection Officer can be contacted at dataprotection@ucem.ac.uk

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.

If you wish to query or withdraw consent for processing then contact the Data Protection Officer at dataprotection@ucem.ac.uk.

4. Data Protection Principles

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

[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.

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 the public task basis 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 2 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. This includes the retention of records of academic achievement.

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. This includes certification with relevant information security standards.

6. 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)?

6.1 Routine data sharing

6.1.1 Data sharing agreements

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

6.1.2 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

6.2 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. 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.

8. 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.

9. 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.

10. 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) or email: casework@ico.gov.uk

Appendix 1: Data Subject Access Requests

1. Who can access information?

UCEM will make sure that only people that need personal information can have access to it. Any data subject can make a Data Subject Access Request (DSAR) about themselves. If a third-party requests information about an individual, the individual must give informed consent to the third party seeking that information.

Students and apprentices

If your fee, or part of your fee is being paid to UCEM by a sponsor, or you are partaking in an apprenticeship programme of studies, information may be released to the sponsor organisation, including your name, date of birth, unique UCEM reference number, programme of study and module details, progress and assessment results.

Staff

Personal information held on staff will only be disclosed to members of the HR department, their own line manager, or a senior manager where specific action is required. If a member of staff accesses the records of another member of staff without authority, this is deemed an act of gross misconduct under our disciplinary policy and is a criminal offence under the DPA 2018.

Trustees

Personal information held on Trustees will only be disclosed to the HR department, members of the Executive Support team who deal with board administration, or Deans or Vice-Principals, should any action need to be taken in relation to conduct.

2. Identity Validation

To ensure that information is only disclosed to people who are entitled to see it the identity of the person requesting the information will be validated before disclosure.

Prospective student/apprentice

When receiving a request for information by any means information will only be disclosed if the following checks are passed:

Either

- a valid application number has been supplied.
- the name supplied matches the name held against the application.
- If an email address is supplied, it must match to an email held against the application

or the following information is supplied and matches to an application:

- Name
- date of birth
- programme applied for

- approximate date of application (+/- 2 years).

Current student/apprentice

When receiving a request for information by post or email information will only be disclosed if the following checks are passed:

- A valid student number has been supplied.
- The name supplied matches the name held against the student number.
- If an email address is supplied, it must match to an email held against the student.

When a request for information is made over the phone the identity of the caller will be verified by:

- Obtaining a valid student number.
- Obtaining a name that matches to the student number.
- Obtaining the name of the programme they are studying.
- If there is any doubt the date of birth should also be checked to confirm identity.

If a student is unable to supply their student number, then the following information should be supplied and should match to the record on SITS before disclosing the student number:

- Full name.
- Email address.
- Date of birth.
- Programme being studied

Past student/apprentice

When receiving a request for information by any means information will only be disclosed if the following checks are passed:

Either

- a valid student number has been supplied.
- the name supplied matches the name held against the student number.
- If an email address is supplied, it must match to an email held against the student.

Or the following information is supplied and matches to a record on the student records system:

- name when studied at UCEM,
- date of birth,
- programme studied,
- approximate date of graduation (+/- 2 years).

Approved Third Party

This is when a student has given permission for a third party to access their information in writing and the approval has been verified as coming from the student.

The third party must provide the following information in all communication and this must match to the information held against the student:

- Student number and/or date of birth
- Student name whilst registered as a student
- Third party name.
- Third party relationship with student.
- Signed/dated authorisation

Former Member of Staff

When receiving a request for information from a current member of staff the request must either come from the staff member's email address or be made in a 1-1 meeting with the staff member, either verbally or by the handing over of a written request.

Past Member of Staff

When receiving a request for information from a past member of staff the person should be requested to supply a full name.

Other Contacts

UCEM holds information on suppliers, course delegates and other people who have worked with UCEM or who are marketed to by UCEM. If a request is received from one of these individuals for information by default provision of a name and address or name and email address that matches our records is viewed as sufficient information to identify them.

3. Making a data subject access request

All UCEM staff are trained in data protection as part of their induction and on an ongoing basis so will be able to recognise a request for personal data and will pass it immediately to the Data Protection Officer at dataprotection@ucem.ac.uk.

How to make the request

The request should be made by the individual (the data subject) unless they have authorised a third party to make the request. The identity validation process set out above will ensure that personal information is only disclosed to someone who has the right to see it.

What you are entitled to

Subject access entitles an individual to more than just a copy of their personal data. An individual is also entitled to be:

- told whether any personal data is being processed – so, if we hold no personal data about the requester, we must still respond to you to let you know this;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and
- given details of the source of the data (if known).

Timescales

The time period for dealing with a DSAR under the DPA 2018 is without undue delay and within one month. The time period starts from the day after the request is received to the corresponding calendar date in the next month. If the following month is shorter it is the last day of the following month. If a corresponding day is a weekend or public holiday it is the next working day.

UCEM will endeavour to respond as soon as possible.

4. Exemptions and refusals

Frequent requests

The DPA 2018 allows some discretion when dealing with requests that are made at unreasonable intervals. It says we are not obliged to comply with an identical or similar request to one we have already dealt with unless a reasonable interval has elapsed between the first request and any subsequent ones.

Although there is no statutory definition of a reasonable interval as it depends on factors such as how often the data is updated, we will generally consider a reasonable interval to be within the last three months. A search of previous requests will be made to ensure that this is not a similar request to one made previously. Legal advice will always be sought if a request is to be refused. The DPA 2018 also provides for refusing on the basis of 'manifestly unfounded or excessive' requests (section 53)

Manifestly unfounded or excessive requests

The courts have determined that there is scope for assessing whether, in the circumstances of a particular case, complying with a request by supplying a copy of the requested information in permanent form would result in so much work or expense as to outweigh the requester's right of access to their personal data.

The courts have also made it clear that in assessing whether complying with a Subject Access Request would involve disproportionate effort we may take into account difficulties which occur throughout the process of complying with the request, including any difficulties we encounter in finding the requested information.

If the request for information is very vague clarification can be sought as to what is being requested. If such clarification is sought this should be noted in the Subject Access log on SharePoint. With manifestly unfounded or excessive requests we have the discretion to charge either a reasonable fee or to refuse to comply with the request.

Exemption for requests for information about the outcome of academic, professional or other examinations

These rules, which apply to requests for examination scripts, marks or markers' comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body's processes for announcing results. Information comprising the answers given by a candidate during an examination is exempt from the right of subject access. A Data Subject Access Request ('DSAR') cannot be used to obtain a copy of an individual's examination script. Although this exemption does not extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of

the marks awarded, there is a special rule governing the time limit for responding to a Subject Access Request for such information in cases where the Subject Access Request is made before the results are announced. In such cases, a response must be provided within the earlier of:

- five months of the date of the request; or
- if earlier, before the end of the period of 40 days beginning with the announcement of the results

(DPA 2018 Schedule 2 Part 4 para 25). Where a request is made for an individual's examination marks, a response may only be refused (or delayed) for reasons permitted by the legislation. We would not refuse to provide details of examination marks in response to a Subject Access Request because the requester, or their sponsor, had failed to pay their tuition fees. Clearly, though, providing information about examination results is not the same as conferring a qualification.

5. What UCEM will do

The request will be logged in the Data Subject Access Request log. The log will record the date and time the request was received, who it was received from, the staff member who received the request and a reference number for the request will be allocated.

Finding the information

The DPO will coordinate the response but may need to contact the Information Champions in each area who will be responsible for searching the records in their area and providing the information to the DPO.

Format and exemptions

The DPO is responsible for deciding what information should be disclosed, what exemptions should be applied (see below) and what format the response should be sent in. UCEM will try to provide information in the format which has been requested but cannot guarantee that this will always be possible or practical.

Where exemptions are applied legal advice will be sought. Possible exemptions include:

- References given (not received)
- Publicly available information
- Management information (such as restructuring or possible redundancies)
- Negotiations with the requestor
- Legal advice and proceedings
- Third party data

Sending the information

A full audit trail will be maintained by the DPO of the systems interrogated, the number of items identified, exemptions applied and how decisions about what should be disclosed have been taken.

When the information is sent the Data Subject Access Request (DSAR) log will be updated with all relevant information.

A copy of the information supplied will be retained by the DPO.

Appendix 2: 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

The Higher Education Access Tracker publishes a Privacy Notice at https://heat.ac.uk/privacy-notice/