UCQ UNIVERSITY CENTRE QUAYSIDE

Data and Privacy Policy

Version: 4
Revision date: 10/02/2020

Due for review: 10/02/2022

Table of Contents

1. Policy statement

1.1 University Centre Quayside (UCQ) respects privacy and is committed to protecting personal data.

1.2 UCQ is required to retain certain information about its employees, students and other users in order to facilitate the monitoring of performance, achievements, and health and safety.

1.3 It is also necessary to process information so that staff can be recruited and paid and education courses and legal obligations to funding bodies, government departments and regulatory bodies complied with. To comply with the law, information stored in files (either paper based or electronically, including e-mail, internet, intranet or portable storage device) are covered by data protection legislation and must be collected and used fairly, stored and disposed of safely, and not disclosed to any other person unlawfully or without consent.

1.4 UCQ must comply with the data protection principles which are set out in the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA). Other relevant policies that feed into this policy include the Freedom of Information Act 2000, Protection of Freedoms Act 2012, Computer Misuse Act 1990 and the Education Act 2011.

1.5 Who we are

1.5.1 University Centre Quayside Limited is a provider of further and higher education in England.

1.6 Data Controller

1.6.1 This Data and Privacy Policy is issued on behalf of University Centre Quayside Limited, so when we mention “UCQ”, “we”, “us” or “our” in this Data and Privacy Policy, we are referring to University Centre Quayside Limited as the entity responsible for processing your data.

1.6.1 This Policy shall apply to any UCQ website including any subdomains that may be made available by us from time to time; including websites with the ending ‘.ucq.ac.uk; and all UCQ social media channels.

1.7 Contact details

1.7.1 We have appointed a Data Protection Officer (“DPO”) who is responsible for overseeing questions in relation to this Data and Privacy Policy. If there are any questions about this Data and Privacy Policy, including any requests to exercise legal rights, please contact the DPO using the following details:

For the attention of the Data Protection Officer
University Centre Quayside Limited
Quayside i4
Albion Row
Newcastle Upon Tyne
NE6 1LL
Email address: ask@ucq.ac.uk

2. Principles

2.1 UCQ and all staff who process data must ensure that the DPA principles are adhered to at all times:

1) The first data protection principle is that the processing of personal data must be:
   - lawful, and
   - fair and transparent

2) The second data protection principle is that:
   - the purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;
   - personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

3) The third data protection principle is that:
   - personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

4) The fourth data protection principle is that:
   - personal data undergoing processing must be accurate and, where necessary, kept up to date.

5) The fifth data protection principle is that:
   - personal data must be kept for no longer than is necessary for the purpose for which it is processed.

6) The sixth data protection principle is that:
   - personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

3. Personal data

3.1 What we may collect, use and store

3.1.1 Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We may collect, use, store and transfer different kinds of personal data which we have grouped together below.

3.2 Audio / Visual Data

3.2.1 Includes recordings from closed circuit televisions systems in place for security purposes at our premises, telephone recordings, video recordings (for example in teaching sessions).

3.3 Contact Data

3.3.1 Includes physical address, email address and telephone numbers.

3.4 Eligibility Data

3.4.1 Includes education history, records of qualifications and/or training, personal statements and references.

3.5 Employment Data

3.5.1 Includes name of employer, job title, work contact details (email address, telephone number and postal address), National Insurance number and employment start and end dates.

3.6 Financial Data

3.6.1 Includes bank account, billing information, payment card details.

3.7 Identity Data

3.7.1 Includes first name, maiden name, last name, student reference numbers, usernames for IT systems, marital status, title, date of birth and gender.

3.8 Marketing and Communications Data

3.8.1 Includes preferences in receiving marketing from us and communication preferences.

3.9 Next of Kin Data

3.9.1 Includes the name and contact information to be used in the event of an emergency.

3.10 Profile Data

3.10.1 Includes usernames and passwords (for UCQ systems), interests, preferences, feedback, survey responses and enquiries submitted to UCQ.

3.11 Recruitment Data

3.11.1 Includes any information provided to us in a curriculum vitae, any covering letter, any application form (including name, title, address, telephone number, personal email address, date of birth, gender, employment history, qualifications and reasons for wanting to apply for the relevant position) and any information provided to UCQ during an interview.

3.12 Student Data

3.12.1 Includes the course or programme being undertaken with UCQ, records of achievements (exam, assessment and achievement results), exam scripts, exam transcripts, attendance and progress information, feedback from staff, emails sent to UCQ, emails sent/received by a UCQ email address or messages posted in a VLE, information relating to your use of library and library resources (including materials checked out and overdue items), information relating to involvement in student associations (including membership of student groups or attendance of student events) , information relating to registration for or attendance at any UCQ hosted/advertised events, information relating to allegations of academic misconduct or other matters of discipline, information relating to any application for mitigating circumstances,

any application for deferrals or interruption of studies and any complaints made to or about you to UCQ.

3.13 Technical Data

3.13.1 Includes internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices that are used to access any UCQ online systems and websites.

3.14 Usage Data

3.14.1 Includes information about a visit to a UCQ website, including the Uniform Resource Locators (URL) clickstream to, through and from the Websites (including date and time), products and/or services you viewed or searched for, page response times, download errors, lengths of visits to certain pages, page interaction information (such as scrolling, clicks and mouseovers) and methods used to browse away from the page and any phone number used to call us.

3.15 Sensitive personal data

3.15.1 Stronger legal protection exists for more sensitive information, defined as 'special category data' which include:

- the racial or ethnic origin of the data subject;
- their political opinions;
- their religious beliefs or other beliefs of a similar or philosophical nature;
- whether they are a member of a trade union;
- their physical or mental health;
- their sexual life or sexual orientation;
- genetic/biometric data processed for the purpose of uniquely identifying a natural person

3.15.2 In some circumstances we may also collect, store and use 'special category data'.

4. How data is collected

4.1 We collect data via a range of methods and sources. Typically, data is collected through direct interactions during which an individual may provide us with identity, contact, employment, financial and marketing and communications data by filling in forms, or by corresponding with us face-to-face, by post, phone, email or otherwise.

4.2 Student data collection

4.2.1 Student data will be collected in the ways listed above and in addition as a result of the student's studies. This includes personal data provided when:

- Attending learning sessions
- Submitting work for assessment
- Taking examinations or other assessments
- Asking questions to UCQ staff
- Engaging with the VLE

4.3 Employee data collection

4.3.1 Employee data is collected as part of the recruitment process and continues throughout the during of employment and, for certain information, for a statutory period after employment ends. The personal data held for employees includes:

- Identity information (name, address, age etc)
- Job application data (education history, employment history, previous salary etc)
- Evidence of their Right to Work in the UK
- Bank account details for payroll purposes
- HR records (such as sickness, lateness, performance/appraisal information etc)

4.4 Third party data

4.4.1 We may receive personal data from various third parties. They include:

- Any organisation referring students to UCQ (DWP, charities etc.)
- Employers
- Government systems (such as LRS, digital apprenticeship service)
- Disclosure and Barring Service (DBS)
- Technical data from analytics providers such as Google.

4.5 Consent

4.5.1 University Centre Quayside will comply with the following guidance surrounding 'consent':

4.5.2 Consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action, consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions and individuals should be provided a simple way to withdraw consent. It must also be verifiable.

5. How we use data

5.1 Data usage within the law

5.1.1 UCQ will only ever use personal data when the law allows. Most commonly, we will use personal data in the following circumstances:

- Where we need to perform a contract we are about to enter into or have entered into with an individual (for example, enrolling a student onto one of our education programmes)
- Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the individual do not override those interests
- Where we need to comply with a legal or regulatory obligation
- Where we have explicit consent

5.1.2 Where we are relying on an individual's consent as the legal basis for processing their data, the individual may withdraw that consent at any time.

5.2 Purposes for using personal data

5.2.1 Our lawful basis for processing your personal data will be, in the majority of cases, to perform our contract with an individual. As an example, students who enrol on a programme have made an agreement with UCQ and provided personal information and data as part of that.

5.3 Sensitive personal information

5.3.1 Special categories of particularly sensitive personal information require higher levels of protection.

5.3.2 We need to have further justification for collecting, storing and using this type of personal information. We have in place this Data and Privacy Policy and safeguards which we are required by law to maintain when processing such data.

5.4 Consent relating to sensitive information

5.4.1 We do not need consent if we use special categories of personal data to carry out our legal obligations.

5.4.2 We may, in certain circumstances, ask for your explicit consent to allow us to process particularly sensitive data. When we do, we will provide individuals with full details of the information that we would like and the reason we need it, so that it can be carefully considered whether consent is to be given.

5.4.3 Individuals will be made aware that it is not a condition of contract with us that you agree to any request for consent. However, we may not be able to provide certain services (such as additional support needs) if such data is not provided to us.

5.5 Change of purpose

5.5.1 We will only use personal data for the purposes for which it was collected, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. We will always provide full justification, information and the legal basis for the change of data use to an individual prior to the change.

5.5.2 Please note that we may process personal data without an individual's knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5.6 Communications

5.6.1 In the situation that an individual has been provided with a UCQ email address (ending with @ucq.ac.uk or @quayside.ac.uk), we will only use this email address to communicate with you in relation to personal data, such as HR information or assessment results in the case of students.

6. Disclosure of personal data

6.1 We may have to share your personal data with the parties set out below for varying purposes:

- Internal Third Parties, defined as other UCQ group organisations.
- External Third Parties such as HMRC, UK Home Office, Department for Education.
- A parent or guardian for persons under the age of 18 (or if it is specifically requested for us to liaise with a parent or guardian).
- External venues where some element of a course or programme (or event) is delivered (UCQ may share Identity Data with the venue for registration and health and safety purposes).
- Counselling services (UCQ may share Identity and Contact Data).
- Academic plagiarism checkers, such as Viper, Turnitin (UCQ may share Identity and Student Data with such systems).
- Future employers or education providers where it is specifically requested that we provide confirmation of Identity or Student Data to those parties for reference purposes.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Data and Privacy Policy.

6.2 We require all third parties to respect the security of personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use personal data for their own purposes and only permit them to process personal data for specified purposes and in accordance with our instructions.

7. The Bribery Act and your data

7.1 UCQ is required to comply with the UK Bribery Act (2010) and any other local laws or regulations relating to similar purposes which relate to fraudulent, illegal or unethical behaviour.

7.2 Personal data will only be used for the purpose of ensuring compliance by UCQ with the relevant laws and regulations. Wherever reasonably possible, personal data will be anonymised prior to use for the purpose of investigations and remedial action so that it does not relate to an individual. However, in some specific circumstances this may not be possible as it may prohibit a full investigation and prevent compliance with a relevant regulation or conduct legislation.

8. Data security and integrity

8.1 UCQ have appropriate security measures in place to prevent personal data from being accidentally lost, used, accessed, altered or disclosed in any unauthorised way. This includes monitored 24 hour incremental backups and full weekly backup cycles, which includes onsite and offsite backups of data and system configurations.

8.2 We regularly review our security measures to ensure they remain up to date, appropriate and robust. In addition, we limit access to personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal data on our instructions and they are subject to a duty of confidentiality.

8.3 We have put in place procedures to deal with any suspected personal data breach and will notify individuals and any applicable regulator of a breach where we are legally required to do so.

8.4 Your personal data may be held on the IT systems of UCQ, and/or on the IT systems of another third-party company (within or outside of UCQ) within or outside the EEA which is providing IT hosting or other data processing services, in accordance with UCQ's arrangement in place with that company.

8.5 All information that you provide to us is stored on secure servers. Where we have given (or where an individual has chosen) a password which enables access to certain parts of the websites, the responsibility is with the individual for keeping this password confidential. We ask people not to share a password with anyone.

8.6 UCQ employee obligations

8.6.1 All UCQ staff will be made aware of this policy and their duties under the DPA. All staff and students are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to personal data.

8.6.2 All staff have responsibility for ensuring that:

- Any personal data which they hold is stored and disposed of securely
- Personal information is not disclosed orally, in writing, accidentally, or otherwise to any unauthorised third party.

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

8.6.4 Personal information must be stored securely, this means:

- In a locked office, or
- In a locked filing cabinet, or
- In a locked drawer, or
- If it is in digital format, the data must only be accessible by an authorised personnel, with appropriate system permissions set. The Personnel must use a private username password upon securely accessing the UCQ computer systems.
- If it is kept on portable storage (i.e. USB, laptop etc..) the device must be encrypted and itself kept securely. This does not include in a locked car.

8.7 Unauthorised access

8.7.1 Any member of staff or student who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party may be disciplined in accordance with UCQ's disciplinary procedures.

9. Data retention

9.1 We will only retain personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

9.2 To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which we process personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

9.3 UCQ may retain data for differing periods of time as required by statute or best practices. Please refer to the UCQ Data Retention Policy for specific guidance surrounding the retention of data.

9.4 In some circumstances, we may anonymise personal data (so that it can no longer be associated with an individual) for research or statistical purposes in which case we may use this information indefinitely without further notice.

10. An individual's legal rights

10.1 Under certain circumstances, individuals have rights under data protection laws in relation to personal data. They are:

- Requesting access to your personal data.
- Requesting correction of your personal data.
- Requesting erasure of your personal data.
- Objecting to the processing of your personal data.
- Requesting restriction of processing your personal data.
- Requesting transfer of your personal data.
- The right to withdraw consent.

10.2 These rights can be exercised at any time by contacting UCQ's Data Protection Officer (see section 1.7).

10.3 Rights of access to information

10.3.1 Should a data subject wish to access their personal data held by UCQ they should contact the Data Protection Officer with details of their request. We would normally expect to respond to requests within one month.

10.4.1 Information requests that fall outside personal data are ordinarily covered under the Freedom of Information Act 2000 (FOI). However, University Centre Quayside is a private limited company and as such is not in scope under the FOI for these types of requests.

10.4 Data accuracy

10.4.1 UCQ will endeavour to ensure that all personal data held is accurate. Staff and students must ensure that all personal data provided to UCQ is correct and up to date. Staff and students must ensure that changes of address, and similar information, are notified to the relevant personnel as soon as possible.