University of Central Lancashire

Data protection policy

Document control information	
Classification	Internal and external
Responsibility for drafting	Information Governance Manager & Data Protection Officer
Consulted with	JNCC; UCLan Community Dentists Limited; Information and Data Governance Group
Approved by	University Secretary & General Counsel
Effective from	3rd October 2024
This version last reviewed on	3rd October 2024
Next review date	As required following legislative or procedural changes
Enquiries to	Information Governance Manager & Data Protection Officer
This document is issued by Legal and Governance. Any copied or printed versions will be an uncontrolled copy. The definitive version is available from the Information Governance Manager & Data Protection Officer: DPFOIA@uclan.ac.uk	

Contents

Data protection policy

A Introduction

During the course of our activities the University and its wholly-owned companies (together, "the University", for the purposes of this policy) collect, use and store personal data about a variety of individuals with whom we have (or have had) contact or whose personal data is otherwise provided to us.

This policy sets out how the University and its wholly-owned companies (with the exception of Training 2000 Limited, which has its own policy) will comply with data protection legislation (the UK General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (the DPA)) and associated legislation. The data protection legislation sets out how personal data should be handled.

This policy is supplemented by guidance which must be followed as part of this policy. This supplementary guidance complements the policy and helps all those to whom the policy applies to comply with its requirements on a practical level. The guidance will be updated as and when necessary and is available to University employees on the Information Governance pages of the staff intranet.

A glossary of terms used throughout this policy is included in section N.

B Scope of the policy

This policy applies to the University's processing of personal data, where processing includes collection; recording; organisation; structuring; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission, dissemination or otherwise making available; alignment or combination; restriction; erasure; or destruction of personal data.

It applies to the processing of personal data about current, past and prospective employees, students and their family members; service providers; suppliers; customers; and any other individuals whose personal data we process. This information may be held on paper or electronically or on other media.

This policy applies to all employees; temporary, casual, contract, agency and ad hoc workers; and any contractors or service providers acting on behalf of the University. These groups are collectively referred to as "colleagues" throughout this policy.

C Policy statement

The University complies with the data protection principles, as set out in section E of this policy, and all other requirements of the data protection legislation whenever it processes personal data. We will provide colleagues with appropriate training in information governance to enable them to comply with, and apply, this policy.

We will establish clear data protection roles and responsibilities and adopt a 'privacy by design' approach when using personal data, conducting data protection impact assessments as required and maintaining a record of our processing activities. We will make appropriate checks to ensure that the processors we use can adequately protect

our personal data and will enter into appropriate contractual arrangements that comply with data protection legislation.

We will adopt processes and procedures to support individuals to exercise their rights under data protection legislation and handle such 'rights requests' in compliance with the data protection legislation. Personal data will be shared with external parties where there is a clear and defined need and a lawful basis to do so, which will – where appropriate – be documented in an information sharing agreement. We will put in place technical and organisational measures to ensure the personal data we process is secure and we will maintain an information governance incident reporting process to ensure that colleagues report personal data breaches and ensure that when they are reported, they are risk-assessed and appropriately managed and remediated.

D Responsibilities

All colleagues must comply with this policy whenever they process personal data in the course of their work for the University.

The University Secretary & General Counsel has overall responsibility for ensuring the University complies with the data protection legislation and this policy.

The Information Governance Manager & Data Protection Officer supports the University Secretary & General Counsel with this responsibility. The Information Governance Manager & Data Protection Officer is responsible for updating this policy as required following legislative or procedural changes, on behalf of the University Secretary & General Counsel.

The Information Governance Manager & Data Protection Officer can be contacted on DPFOIA@uclan.ac.uk and will respond to questions or concerns about the operation of this policy and consider any amendments to the policy that are recommended.

The University will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives and that it reflects the requirements of applicable data protection legislation.

E Data protection principles

When processing personal data, colleagues will comply with the six data protection principles set out in the UK GDPR. We will ensure that we are able to demonstrate, through our day-to-day operations, how we comply with these principles. The principles are summarised below and require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner

Compliance with the data protection legislation helps to ensure that personal data is processed fairly and in a transparent manner and without adversely affecting the rights of the data subject. We will tell data subjects who the controller is (for most of our purposes, this will be the University of Central Lancashire), the purposes for which the data are to be processed and the identities of any other parties to whom the data may be disclosed or transferred, among other things. This information will be provided to the data subject in a

privacy notice at the time the data is collected or as soon as practically possible afterwards.

We will process personal data lawfully by ensuring there is a lawful basis from the UK GDPR for all the processing we undertake. When special category data or data about criminal convictions is being processed, we will ensure that an additional lawful basis applies. In all cases, consent as a lawful basis will only be relied upon where consent is fully informed and can be freely given and withdrawn.

2. Processed for limited purposes

We will only process personal data for the specific purposes notified to the data subject via the privacy notice when the data was first collected or for any other purposes permitted under the data protection legislation. Personal data will not be further processed in a manner which is incompatible with these purposes. If it becomes necessary to change the purpose for which the data is processed and that change is incompatible with the original stated purpose, data subjects will be informed of the new purpose before any processing occurs.

3. Adequate, relevant and not excessive (data minimisation)

We will ensure that we process sufficient personal data for the purposes for which it is held. Information which is not needed or is not relevant for a purpose will not be collected or otherwise processed. The minimum amount of personal data needed to properly achieve the purpose in question will be identified and collected; additional, excessive personal data will not be held.

4. Accurate and up-to-date

We will adopt processes, procedures and systems to help ensure that the personal data we process is accurate and, where necessary, kept up-to-date.

Personal data identified as being factually inaccurate will – where appropriate - be amended or erased; however it may not be appropriate to delete this information altogether if historic decisions have been based on it. In these cases, the information will be rectified for future use with an explanatory note placed on file as required to explain the situation. Where a data subject disagrees with a professional opinion about themselves which does not – by definition – constitute verifiable fact, the data subject's difference of opinion will be recorded.

5. Not kept for longer than is necessary (storage limitation)

We will not keep personal data for longer than is necessary for the purposes for which is it being processed. We will securely destroy or erase personal data from our systems when it is no longer required. The exception is personal data that has historical value, which will be considered for transfer to the University Archive for permanent preservation.

We will manage personal data in line with the University's Information Management Policy and Retention Schedule, which provide guidance on how long certain types of record should be retained and when and how they should be destroyed. We will advise colleagues to consult the Information Governance pages of the staff intranet for the current guidance.

6. Secure (integrity and confidentiality)

We will ensure that appropriate technical and organisational security measures are in place to protect against unlawful or unauthorised processing of personal data and against the accidental loss or destruction of, or damage to, personal data (see section F).

F Security of personal data

We will put in place procedures and technologies to maintain the security of the personal data we process from the point of collection to the point of destruction. We will develop procedures and guidance and use fit for purpose technology that will help us to ensure that:

- Only people who are authorised to use personal data will be able to access it.
- Personal data will be protected from unauthorised changes.
- Personal data is available to authorised colleagues when it's needed.

Colleagues who process personal data in the course of their work for the University will follow the policies and guidance published on the Information Governance intranet pages in relation to the processing and management of personal data, and also any service-, school-, or company-specific procedures and guidance which set out how to handle personal data processed in those work areas.

G Using processors

Personal data will only be accessible to a processor if that processor can provide sufficient guarantees that it can put in place appropriate technical and organisational measures to comply with data protection legislation to protect the rights of data subjects and ensure our personal data remains secure. Colleagues responsible for engaging the services of a processor will ensure that appropriate due diligence checks are undertaken to ensure any proposed processors can provide such guarantees.

We will put in place processes, procedures and guidance to help ensure that processors will only be used if the processing is carried out under a binding contract or other legal act which, in either case, meets the requirements of Article 28 UK GDPR.

H International transfers

We will not transfer personal data to a country or territory outside the UK unless:

- The UK Government has determined that the country or territory offers an adequate level of protection and has issued an adequacy decision stating the same; or
- Appropriate safeguards are in place, such as binding corporate rules or standard data protection clauses issued by the UK Information Commissioner; or
- One of the conditions set out in Article 49 UK GDPR applies.

In all cases, colleagues will follow internal guidance and where necessary, seek advice from the Information Governance Manager & Data Protection Officer before transferring any personal data to a country outside the UK.

I Individuals' rights

We will adopt processes and procedures to support individuals to exercise their rights under data protection legislation and handle such 'rights requests' in compliance with the data protection legislation. These individual rights include the following:

- The right to be informed
- The right of access (subject access requests)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling.

Colleagues will be trained on how to recognise requests from data subjects to exercise their individual rights and will forward any such requests to the Information Governance team without delay, to be handled in line with the requirements of the UK GDPR. The exception is requests from data subjects made to UCLan Community Dentists Limited, which may be dealt with directly by the UCLan Community Dentists Clinic Manager.

J Formal requests for personal data

Subject access requests

We will assist individuals wishing to make a subject access request and will – on request - provide individuals with a copy of the personal data to which they are entitled. We will make appropriate checks to ensure we are satisfied as to the identity of the data subject. Information will be provided electronically, where possible, and within one calendar month.

We will accept subject access requests made in writing or verbally. Any colleague who receives a subject access request directly from another individual will forward it to the Information Governance team without delay by email to DPFOIA@uclan.ac.uk. The request will be recorded and logged with a unique reference number. The Information Governance team will coordinate and prepare responses to subject access requests and will provide advice and guidance to colleagues who are involved in handling the request. Subject access requests made in relation to personal data for which UCLan Community Dentists Limited is the controller may be dealt with directly by the UCLan Community Dentists Clinic Manager.

Requests from third parties for disclosure of information

When we receive a request for personal data from a third party such as solicitors, the police, the DWP, local authorities, NHS or insurance companies asking for information about a student, employee or other third party e.g. someone caught on CCTV footage and the third party is not acting on the data subject's behalf, we will only consider such requests when they are made in writing. No personal data will be disclosed unless it can be disclosed in compliance with data protection legislation.

During normal business hours, all such requests will be dealt with by the Information Governance team and will not be responded to by other colleagues directly without taking advice from the Information Governance team. Colleagues receiving such requests from third parties will direct them to put their request in writing to the Information Governance team. Out of normal business hours or in an emergency, these requests may be dealt with by the Security team or the on-call Wellbeing teams within Student Services. Where appropriate, requests may also be dealt with directly by the UCLan Community Dentists Clinic Manager.

K Information governance incidents

Colleagues who cause or become aware of an actual or suspected personal data breach (also known as an information governance incident) will inform the Information Governance team immediately so that remedial action can be taken to protect data subjects who may be affected and preserve the reputation of the University. Reports will be made using the breach reporting form on the intranet, by email or by telephone or Teams call. If a potential security breach also involves IT equipment, the UCLan network or emails, colleagues will also inform the IT Security Manager immediately via extension 5355 or by email to LISCustomerServices@uclan.ac.uk

We will assess reported breaches without delay and report any significant breaches to the Information Commissioner within 72 hours of becoming aware of them, where data protection legislation requires this. We will also inform affected data subjects, where data protection legislation requires this.

L Using personal data for personal matters

Colleagues who have access to personal data during the course of their work for the University shall not use University-controlled personal data for their own purposes. Colleagues are in a position of trust and shall not abuse that position to access personal information for non-University purposes. Colleagues must only access or otherwise process University-controlled personal data for University business purposes and not for personal curiosity or any other unofficial or unauthorised purpose.

Any person who knowingly or recklessly obtains or discloses University-controlled personal data without the University's consent is committing a criminal offence under data protection legislation and can face prosecution under the data protection legislation.

M Breach of the policy

This policy is based on the requirements of the data protection legislation; therefore breach of the policy may be a breach of the law. If you are concerned that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with the Information Governance Manager & Data Protection Officer.

Negligent, reckless or deliberate breaches of data protection legislation which are likely to cause substantial damage or substantial distress may lead to the University being issued with a fine of up to £17.5 million by the Information Commissioner's Office. Compliance with this policy will minimise the likelihood of this occurring.

We will investigate actual or potential breaches of this policy that we become aware of. Any investigation may result in disciplinary action or dismissal, where appropriate.

N Glossary of terms

Personal data	Data relating to a living individual who can be identified from that data (or from that data and other information in our possession or likely to come into our possession). Personal data can be factual (such as name, address, date of birth) or it can be an opinion (such as aspects of an employment reference). Information can be personal data without including a person's name.
Special category data and criminal offence data	Special category data is information about a person's: • Racial or ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Trade union membership; • Genetic data; • Biometric data used to uniquely identify someone; • Health data • Sexual life or sexual orientation. Information relating to actual or alleged criminal offences or convictions, and any proceedings in relation to the same, is treated in a similar way to special category data. Processing these types of information is prohibited unless certain legal bases apply.
Data subject	The individual the personal data relates to.
Controller	The person or organisation which, alone or jointly with others, determines how and why personal data will be used. UCLan is a controller.
Processor	A person or organisation which processes personal data on behalf of the controller.
Colleague or Colleagues	All employees; temporary, casual, contract, agency and ad hoc workers; and any contractors or service providers acting on behalf of the University.
Personal data breach	A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Privacy notice	A statement provided to data subjects when or before their personal data is collected which explains who the controller is, what their personal data will be used for, to whom it may be disclosed for these purposes and any other information they may need to know in order to ensure that the processing is fair, as set out in Article 13 and 14 UK GDPR.
Information Commissioner	An independent regulator who reports directly to Parliament. The Information Commissioner is responsible for regulating and enforcing data protection legislation in the UK and provides advice and guidance about compliance to organisations and members of the public.