University of Central Lancashire

Data protection policy

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

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

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

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

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