University of Central Lancashire

Data Protection Policy

Effective October 2015 - Present

STUDENT REGULATIONS AND POLICIES

uclan.ac.uk/studentcontract

UNIVERSITY OF CENTRAL LANCASHIRE

Data Protection Policy

Contents

UNIVERSITY OF CENTRAL LANCASHIRE
DATA PROTECTION POLICY

A Introduction

Everyone has rights regarding the manner in which their personal data is handled. During the course of our activities we will collect, store and otherwise process personal information about a variety of individuals with whom we have (or have had) contact.

This policy is supplemented by guidance documents which must also be adhered to as part of this policy. This supplementary guidance is designed to complement the policy and help those subject to the policy to comply with its requirements on a practical level. The guidance will be updated as and when necessary.

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

B Scope of the Policy

This policy sets out the University's requirements regarding data protection and the legal conditions which must be satisfied in relation to the processing of personal data, where processing includes obtaining, recording, holding, altering, disclosing, destroying or otherwise using personal data.

The types of information that we may be required to handle include details of current, past and prospective employees and students and their family members, service providers, suppliers, customers and any others with whom we communicate. This information may be held on paper or on a computer or other media and is subject to certain legal safeguards specified in the Data Protection Act 1998 (the DPA) and other regulations. The DPA sets out how that information should be handled and imposes restrictions on how we may use it.

C Policy statement

The University of Central Lancashire takes its responsibilities under the DPA and the requirement to treat personal information in an appropriate and lawful manner very seriously and as such, complies with the data protection principles, as set out in section E of this policy.

D Responsibilities

This policy applies to all employees, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of the University.

The Chief Operating Officer (COO) has overall responsibility for ensuring the University complies with the DPA and with this policy. The COO is supported in this responsibility by the Information Governance Officer, who is based in Legal Services and can be contacted on DPFOIA@uclan.ac.uk or extension 2561. Any questions or concerns about the operation of this policy should be referred in the first instance to the Information Governance Officer.

This policy is reviewed annually by the Information Governance Officer, on behalf of the COO. Recommendations for any amendments should be reported to the Information Governance Officer

for consideration as part of the review process. The University will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

E Data protection principles

Employees processing personal data must comply with the eight data protection principles. These are principles of good practice and compliance is a requirement of the DPA, enforced by the Information Commissioner. The principles are summarised below and require that personal data must be:

1. Processed fairly and lawfully

The DPA is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (for most of our purposes, this will be the University of Central Lancashire), the purpose for which the data are to be processed and the identities of any other parties to whom the data may be disclosed or transferred. This information must be provided to the data subject in a privacy notice at the time the data is collected or if this is not possible, then as soon as is practicable.

For personal data to be processed lawfully, certain conditions must be met. These may include obtaining the data subject's consent to the processing or ensuring the processing is necessary for the legitimate interests of UCLan or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In most cases the data subject's explicit consent will be required. In all cases, consent must only be sought where it can be freely given and withdrawn; if something is a legitimate mandatory or legal requirement, data subjects should not be asked for consent and given the impression that they have a choice if this is not the case. Advice from the Information Governance Officer (DPFOIA@uclan.ac.uk) should be sought on consent issues and before processing sensitive personal data.

2. Processed for limited purposes

Personal data may only be processed for the specific purposes notified to the data subject via the privacy notice when the data was first collected or for any other purposes specifically permitted under the DPA. Personal data must not be further processed in a manner which is incompatible with these purposes. This means that personal data must not be collected for one purpose and then used for an entirely different, unrelated purpose. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs, unless an exemption from this requirement applies. It may be the case that you cannot use the personal data for another purpose unless the data subject consents. Advice should be sought from the Information Governance Officer (DPFOIA@uclan.ac.uk).

3. Adequate, relevant and not excessive

Personal data held about data subjects must be sufficient for the purposes for which it is held. Information which is not needed or is not relevant for a purpose must not be collected or otherwise processed. The minimum amount of personal data needed to properly achieve the purpose in question should be identified and collected; additional, excessive personal data must not be held.

4. Accurate and up-to-date

Personal data must be accurate and, where necessary, kept up-to-date. Information which is incorrect or misleading is not accurate; steps must be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

Personal information identified as being factually inaccurate must be amended; however it may not be appropriate to delete this information altogether if historic decisions have been based on it. In these cases, the information must be amended 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 him or herself which does not – by definition – constitute verifiable fact, the data subject's difference of opinion will be noted on the file in the relevant places.

5. Not kept for longer than is necessary

Personal data must not be kept longer than is necessary for the purpose for which is it being processed. This means that data must be securely destroyed or erased from our systems when it is no longer required i.e. there is no legal requirement to retain it and there is no business or operational need for the information.

Personal information should be managed in line with the University's Records Management Policy and Retention Schedule, which provide guidance on how long certain types of information should be retained and when and how they should be destroyed. See the Information Governance pages of the UCLan intranet for the current guidance.

6. Processed in line with data subjects' rights

Personal data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any personal data held about them by the University
- Prevent the processing of their data for direct marketing purposes
- Apply to a court to have inaccurate data amended, blocked, erased or destroyed
- Prevent processing that is likely to cause substantial damage or substantial distress to themselves or anyone else
- Require the University to ensure that decisions which significantly affect them are not taken solely based on the processing of personal data by automatic means
- Make a complaint to the Information Commissioner about the way UCLan has processed their personal data.
- Apply to the courts for compensation if they have suffered damage and distress as a result of a contravention of the DPA.

7. Secure

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data (see section F for further information). Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

8. Not transferred to a country outside the EEA unless that country has adequate data protection measures in place

Personal data must not be transferred to a country outside the EEA unless that country has adequate measures in place to ensure that the rights and freedoms of data subjects are protected when their personal data is processed. There are some instances in which this principle does not apply, which include cases where the data subject has consented to the transfer; the transfer is necessary for the performance of a contract between the data subject and UCLan; the transfer is necessary for the purposes of legal proceedings or obtaining legal advice; the transfer is to a country which the European Commission has found to offer an adequate level of protection; or adequate safeguards are put in place using EU Model Contract Clauses. This is not an exhaustive list and employees must seek guidance from the Information Governance Officer before transferring personal data overseas.

F Security of personal data

The DPA requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Maintaining data security means, amongst other things, guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- *Confidentiality* means that only people who are authorised to use data can access it
- *Integrity* means that personal data must be accurate and suitable for the purpose for which it is processed
- *Availability* means that authorised users must be able to access the data if they need it for authorised purposes. Personal data must therefore be stored on the University's secure network with appropriate access controls and not on individual computers, laptops or other devices such as phones, iPads, CDs or memory sticks.

Security procedures include:

- *Vigilance.* Any stranger seen in non-public areas must be questioned (if it is safe to do so) or reported to Security on extension 2068 or securityservice@uclan.ac.uk or if an emergency, dial 333 from an internal line.
- *Entry controls.* Buildings, offices or other secure areas must be locked when empty or not in use. Entry codes must not be shared with unauthorised individuals and keys must be kept secure.
- *Secure lockable desks and cupboards.* Desks, cupboards and filing cabinets must be kept locked if they hold confidential information of any kind. It should always be assumed that personal data is confidential, although there may be cases where it is not.
- *Methods of disposal.* Paper documents containing personal data must be disposed of securely via the University's confidential waste service. They must not be discarded with regular waste or recycling material. Electronic data or media such as USB sticks, CDs, DVDs etc. must be wiped or destroyed securely in line with LIS guidance to ensure that the information is no longer accessible or recoverable. Hardware and devices such as laptops, PCs, smartphones etc. must be cleaned and/or securely disposed of in line with LIS guidance to ensure that the information stored on them is no longer accessible or recoverable. This kind of equipment must only be disposed of in line with LIS guidance and never via normal recycling or waste services.

- *Equipment.* Data users must ensure that individual monitors are positioned in suitable locations to ensure that confidential information is not visible to passers-by or other unauthorised individuals e.g. through office windows or doors. Users must lock their PCs and other devices when they are left unattended, even for a few minutes, to prevent unauthorised access to systems. At the end of each day, users must log out of systems and shut down machines to maintain security and enable essential system updates to be installed. Fax machines must be in secure locations where received faxes are not accessible to unauthorised individuals. Portable equipment such as smartphones, laptops, iPads, or removable media such as USB sticks, CDs etc. must be kept secure and not left unattended in cars, on public transport or in public areas.

- *Preventing disclosure to unauthorised third parties.* Personal data must not be disclosed to unauthorised third parties intentionally or through negligent actions. Personal data must not be disclosed to third parties unless it has been verified that they have authority to access that information. Care must be taken when transmitting personal data e.g. by email or fax to ensure it is addressed correctly, marked appropriately e.g. 'private and confidential' and is only sent to the intended recipient.

Any member of staff working away from UCLan premises will ensure that their working practices comply with the DPA and have due regard for the security and proper management of personal data, as well as their personal safety. All such employees will comply with the guidance supplementary to this policy and any other applicable UCLan guidance and policy.
The University's security guidance, home and mobile working guidance (supplementary to this policy) and the LIS IT Security Policy must be complied with at all times when processing personal data.

Using data processors

There may be times when employees want or need to use the services of a data processor. Personal data must only be transferred to a data processor if that data processor agrees to comply with the University's security and data protection procedures and policies or if he puts in place equivalent measures himself, which we deem to be acceptable.

Data processors must only be used if the processing is carried out under a contract made or evidenced in writing, where that contract states that the data processor is to act only on instructions from UCLan as the data controller and requires the data processor to comply with equivalent technical and organisational security measures to UCLan.

Telephone enquiries

Any employee dealing with telephone enquires must be aware of security requirements and ensure that personal data held by UCLan is not disclosed inadvertently or inappropriately. This applies whether the purpose of the call is a formal request for information or an everyday enquiry. 'Blaggers' can target organisations which hold large amounts of personal data in an attempt to obtain information by deception and employees must be aware of the need to have appropriate security measures in place to prevent this, particularly during telephone calls. In particular employees must:

- Check the caller's identity to make sure that information is only given to or discussed with a person who is entitled to it e.g. if a caller says they are acting on behalf of a student and asks

for an update on a complaint, check that the student has authorised us to liaise with the caller and that the caller is who they say they are; or if a student or employee calls asking about their own information, ask security questions to verify that they are who they say they are.

- Make appropriate security checks if a caller is asking to be provided with personal data. To maintain the security of personal data, employees should suggest that the caller puts their request in writing if they are unsure about his or her identity and whether or not they are entitled to the information. See section G for further information.

- Always ask the Police and other callers to put their request in writing to the Information Governance Officer if they are making a formal request for disclosure of personal information e.g. from the Police, DWP, local authorities etc. See section G for further information about these types of requests.

G Formal requests for personal data

Dealing with subject access requests

The DPA gives individuals the right to access all the personal data a data controller processes about them. This is the right of subject access and UCLan will assist individuals wishing to make a subject access request. Individuals are entitled to be provided with any information which constitutes their personal data unless the information is exempt. These requests must be dealt with in line with the provisions of the DPA and UCLan policy and employees should seek advice where necessary.

Subject access requests must be made in writing. Any employee who receives a subject access request directly from another individual must forward it to the Information Governance Officer without delay (DPFOIA@uclan.ac.uk). The request will then be recorded and logged before sending to the appropriate school or service for action.

No personal data will be provided in response to a subject access request until we are satisfied as to the identity of the data subject.

Dealing with requests from third parties for disclosure of information

Third party organisations or individuals such as solicitors, the police, DWP, local authorities, NHS or insurance companies may make requests to the University for personal information which we hold. This could be information about a student, an employee or other third party e.g. someone caught on CCTV footage. In these cases, the third party will be asking for information about an individual but they are **not** acting on that person's behalf. UCLan will only consider such requests when they are made in writing and no personal data will be disclosed unless it can be disclosed in compliance with the DPA. All such requests must be dealt with by the Information Governance Officer and must not be responded to by other employees directly without taking advice. Employees receiving such requests from external third parties must direct them to put their request in writing to the Information Governance Officer (DPFOIA@uclan.ac.uk).

Employees must not be pressured into disclosing personal data. They must refer to their line manager and/or the Information Governance Officer for advice if they are unsure whether or not it is appropriate to disclose information. Where formal requests for disclosure of personal data are discussed by phone, employees must take note of the requirements set out in section F.

H Using personal data for personal matters

Employees and other data users must not use UCLan-controlled personal data for their own purposes. Employees and other data users are in a position of trust and must not abuse that position to access personal information for non-UCLan purposes. Employees and other data users must access or otherwise process personal data only for UCLan business purposes and not for personal curiosity or any other unofficial purpose.

Any person who knowingly or recklessly obtains or discloses personal information without UCLan's consent is committing a criminal offence under the DPA.

I Breach of the policy

This policy is based on the legal requirements of the DPA; 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 Officer (DPFOIA@uclan.ac.uk).

If you have caused or become aware of an actual or suspected security breach involving personal data e.g. accidental or unintentional disclosure to an unauthorised party, you must inform the Information Governance Officer immediately so that remedial action can be taken to protect data subjects who may be affected and preserve the reputation of the University. If a potential security breach also involves IT equipment, the UCLan network or emails, you should also inform the IT Security team immediately via extension 5355 or LISCustomerSupport@uclan.ac.uk.

In cases of an actual or suspected breach of the DPA which compromises the security of personal data, it is imperative that these are reported without delay so that action can be taken to minimise the risk to data subjects and protect those who may be affected, where necessary. Where security breaches are reported and addressed quickly, the possible consequences to data subjects and to the University's reputation can be minimised.

Negligent, reckless or deliberate breaches of the DPA which are likely to cause substantial damage or substantial distress may lead to the University being issued with a monetary penalty of up to £500,000 by the Information Commissioner's Office. Compliance with this policy will minimise the likelihood of this occurring; however actual or potential breaches of the policy will be treated seriously by the University and will be subject to a full investigation. Any investigation may result in disciplinary action or dismissal, where appropriate.

J Glossary of Terms

Data	Information which is stored electronically (on any media), on a computer (including in emails) or in most non-electronic filing systems or other manual records.
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. Personal data may also be referred to as 'personal information'.
Sensitive personal data	Information about a person's: • Racial or ethnic origin; • Political opinions; • Religious or similar beliefs; • Trade union membership; • Physical or mental health or condition; • Sexual life; or information about • The commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in any such proceedings. *Sensitive personal data* can only be processed under strict conditions and will usually require the explicit consent of the person concerned.
Processing	Any activity which involves the data. It includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Data subject	The individual the data relates to and for the purpose of this policy, data subjects include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
Data controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A data controller must be a 'person' recognised in law i.e. individuals, organisations and other corporate and unincorporated bodies of persons. UCLan is a data controller.
Data processor	Any individual or organisation which processes personal data on behalf of a data controller. Employees of a data controller are not considered to be data processors; however the definition is likely to include suppliers or service providers which handle personal data on a data controller's behalf.
Data user	Includes employees and other staff members whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.
Privacy notice	A statement provided to data subjects when or before their personal data is collected which explains who the data controller is, what their information will be used for, to whom it may be disclosed for these purposes (particularly any external third parties) and any other information they may need to know in order to ensure that the processing is fair.
Information Commissioner	An independent regulator who reports directly to Parliament. The Information Commissioner is responsible for regulating and

	enforcing the DPA in the UK and provides advice and guidance about compliance to organisations and members of the public.