University of Central Lancashire

Data protection policy

Approved: August 2018

Document control information

Classification	Internal and external
Responsibility for drafting	Information Governance Manager & Data Protection Officer
Consulted with	Directorate; JUCC; Information Security and Data Quality Group
Approved by	Pro Vice-Chancellor (Corporate Development) & Registrar
Effective from	August 2018
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

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 terms used throughout this policy is included in section L.

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 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.

We may be required to process a variety of information about current, past and prospective employees and students and their family members, service providers, suppliers, customers and any others with whom we have contact. This information may be held on paper or electronically or on other media and is subject to certain legal safeguards specified in data protection legislation (the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (the DPA)) and other regulations. The data protection legislation 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 data protection legislation 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, and all other requirements of the data protection legislation.

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 University Secretary & General Counsel has overall responsibility for ensuring the University complies with the data protection legislation and with this policy. The University Secretary & General Counsel is supported in this responsibility by the Information Governance Manager & Data Protection Officer, based in Legal and Governance, 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 Manager & Data Protection Officer.

This policy is reviewed and updated by the Information Governance Manager & Data Protection Officer as required following legislative or procedural changes, on behalf of the University Secretary & General Counsel. Recommendations for any amendments should be reported to the Information Governance Manager & Data Protection 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

When processing personal data, anyone to whom this policy applies will comply with the six data protection principles. These are principles of good practice and compliance is a requirement of the data protection legislation, enforced by the Information Commissioner. The principles are summarised below and require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner

The data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and in a transparent manner and without adversely affecting the rights of the data subject. The data subject will be told 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.

UCLan will process personal data lawfully by ensuring there is a legal basis for all the processing we undertake. This may include ensuring the processing is necessary for the performance of a contract, 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 special category data or data about criminal convictions is being processed, we will ensure that an additional legal basis applies. In many cases the data subject's explicit consent will be required to process special category data. In all cases, consent as a legal basis will only be relied upon where consent is fully informed and can be freely given and withdrawn; if the processing is a legitimate mandatory or legal requirement or necessary for the performance of a contract, data subjects will 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 Manager & Data Protection Officer will be sought on consent issues and before processing special category data.

2. Processed for limited purposes

Personal data will 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 data protection legislation. Personal data will not be further processed in a manner which is incompatible with these purposes. This means that personal data will 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 will be informed of the new purpose before any processing occurs. It may be the case that we cannot use the personal data for another purpose unless the data subject consents. Advice will be sought from the Information Governance Manager & Data Protection Officer.

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

Personal data held about data subjects will be sufficient 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

Personal data will be accurate and, where necessary, kept up-to-date. Information which is incorrect or misleading is not accurate; steps will 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 will 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 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 (storage limitation)

Personal data will not be kept longer than is necessary for the purposes for which is it being processed. This means that data will 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, taking account of the purposes for which it was originally requested.

Personal information will be managed in line with the University's Information 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. Staff will consult the Information Governance pages of the UCLan intranet for the current guidance.

6. Secure (integrity and confidentiality)

We will 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).

F Security of personal data

Data protection legislation 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. We will maintain data security by, 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 will be able access it

- *Integrity* means that personal data will be accurate and suitable for the purpose for which it is processed

- *Availability* means that authorised users will be able to access the data if they need it for authorised purposes. Personal data will 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, discs or memory sticks; nor shall it be stored in cloud-based storage solutions unless a solution has been approved for use by the University.

Security procedures include:

- *Vigilance.* Any stranger seen in non-public areas will be questioned (if it is safe to do so) or reported to Security on extension 2068 or security@uclan.ac.uk or if an emergency, dial 333 from an internal line.

- *Entry controls.* Buildings, offices or other secure areas will be locked when empty or not in use. Entry codes will not be shared with unauthorised individuals and keys will be kept secure.

- *Secure lockable desks and cupboards.* Desks, cupboards and filing cabinets will be kept locked if they hold confidential information of any kind. It will 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 will be disposed of securely via the University's confidential waste service. They will not be discarded with regular waste or recycling material. Electronic data or media such as USB sticks, CDs, DVDs etc. will 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. will 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 will only be disposed of in line with LIS guidance and never via normal recycling or waste services.

- *Equipment.* Data users will 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 will 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 will log out of systems and shut down machines to maintain security and enable essential system updates to be installed. Fax machines will 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. will be kept secure and not left unattended in cars, on public transport or in public areas.

- *Preventing disclosure to unauthorised third parties.* Personal data will not be disclosed to unauthorised third parties intentionally or through negligent actions. Personal data will not be disclosed to third parties unless it has been verified that they have authority to access that information. Care will 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.

When working away from UCLan premises, any person to whom this policy applies will ensure that their working practices comply with the data protection legislation and have due regard for the security and proper management of personal data, as well as their personal safety. All such individuals 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 will be complied with at all times when processing personal data.

Using data processors

There may be times when data users want or need to use the services of a data processor. Personal data will only be transferred 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 personal data remains secure.

Processors will only be used if the processing is carried out under a binding contract or other legal act, where that contract sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The contract will also stipulate that the processor is to act only on instructions from UCLan as the controller and will meet all other requirements of Article 28 GDPR.

Telephone enquiries

Any data user dealing with telephone enquires will be aware of security requirements and will 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 will be aware of the need to have appropriate security measures in place to prevent this, particularly during telephone calls. In particular data users will:

- 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, data users will 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, data users will 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, data users will 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 I for further information.

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

G International transfers

Personal data will not be transferred to a country outside the UK or European Economic Area (EEA) unless the transfer is in accordance with data protection legislation. Data protection legislation allows the transfer of personal data to countries outside the UK and EEA in, among others, the following circumstances:

- The European Commission has decided that the country or territory offers an adequate level of protection.
- The controller has provided adequate safeguards, including enforceable data subject rights and effective legal remedies. These adequate safeguards can be achieved by, among other things, binding corporate rules or standard data protection clauses approved by the European Commission.
- The data subject provides his or her explicit consent.
- The transfer is necessary in relation to a contract or legal claim, as long as the transfer is only occasional i.e. not regular or systematic.
- The transfer is necessary to protect the vital interests of a person i.e. a life or death situation, and they are physically or legally incapable of giving consent.

In all cases, data users 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 or EEA.

H Individuals' rights

The University recognises the rights individuals have under data protection legislation and will respect and comply with these rights whenever we process personal data. This includes 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.

I Formal requests for personal data

Dealing with subject access requests

Data protection legislation gives individuals the right to access all the personal data a 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, among other things, a copy of any information which constitutes their personal data unless the information is exempt from disclosure. Information will be provided electronically, where possible. These requests will be dealt with in line with the provisions of the data protection legislation and UCLan policy and data users will seek advice from the Information Governance Manager & Data Protection Officer.

Subject access requests can be made in writing or verbally. Any data user 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 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 unless 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 data protection legislation. All such requests will be dealt with by the Information Governance team and will not be responded to by other data users directly without taking advice from the Information Governance team. Data users receiving such requests from external third parties will direct them to put their request in writing to the Information Governance team.

Data users will not be pressured into disclosing personal data. They will refer to their line manager and/or the Information Governance Manager & Data Protection 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, data users will take note of the requirements set out in section F.

J Using personal data for personal matters

Employees and other data users will not use UCLan-controlled personal data for their own purposes. Employees and other data users are in a position of trust and will not abuse that position to access personal information for non-UCLan purposes. Employees and other data users will 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 data protection legislation.

K Breach of the policy

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

If an employee or other data user has caused or become aware of an actual or suspected security breach involving personal data e.g. accidental or unintentional disclosure to an unauthorised party, they will inform the Information Governance Manager & Data Protection 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, data users will also inform the IT Security team immediately via extension 5355 or by email.

In cases of an actual or suspected breach of data protection legislation which compromises the security of personal data, it is imperative that these are reported to the Information Governance Manager & Data Protection Officer 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. The University 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.

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 monetary penalty of up to €20,000,000 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.

L 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'.

Special category data	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.
Processing	Any activity which involves the data. It 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.
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/Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. UCLan is a data controller.
Data processor/Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data user	Anyone who is subject to this policy and uses personal data, including employees and other staff members, contractors, etc. set out in section D. 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, as set out in Article 13 and 14 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.