Data Protection Code of Practice

Version – v8 – February 2026

Procedure Author – Head of Legal Services
Procedure Owner – Vice Principal (Governance) and University Secretary
Parent Policy Statement – Corporate Governance Policy Statement
Public Access or Staff Only Access – Public
Version – Version 8 – February 2026
Changes and Reason for Changes – Change to documentation required when accessing CCTV, additional CCTV in School of CEPS, two new guides on Gen AI and Real-World Data Testing and change of job titles.

Introduction

The University is committed to the principles and obligations set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We must also make sure we carry out our work in line with the UWS values of Integrity, Respect, Inclusivity and Accountability. We take our responsibilities for data privacy seriously and make sure we hold ourselves accountable for how we process any personal data we hold.

This Code of Practice is in place to make sure everyone understands the way in which data protection applies to their roles within the University. It also makes sure we meet the requirements set out in Article 24(2) of the UK GDPR which requires the University, as a data controller, to have in place an appropriate data protection policy to make sure we meet our obligations under the legislation.

This Code of Practice and the related guidance apply to all staff and students processing personal data. It also applies to any third parties who process data on our behalf.

Any processing of personal data in the University must be in line with this Code of Practice and any related guidelines. All staff and students within the University have a responsibility to ensure that personal data is processed in accordance with the legislation and to seek appropriate guidance from Legal Services if they are not sure of how the legislation or this Code of Practice applies to the work they are doing.

Any breach of the legislation not only has a potential reputational impact for the University but also means we may be subject to a fine imposed by the Information Commissioners Office (ICO) who is the body responsible for enforcing the data protection legislation in the UK.

Any personal or non-employment related use by staff, of personal data held by the University, constitutes a disciplinary offence, up to and including dismissal.

Definitions

In order to be able to understand this Code of Practice it is important to understand some of the key concepts set out in the UK GDPR: -

A ‘data controller’ is the entity who determines the purposes and means of processing personal data.

A ‘data processor’ is the entity responsible for processing personal data on behalf of a controller.

A ‘data subject’ is a natural person whose personal data is processed by a data controller or a data processor.

‘personal data’ means any information relating to an identified or identifiable person, for example, the name, date of birth or nationality of a person (and includes sensitive personal data).

'sensitive personal data' means a special category of data where additional care is required when you are processing this and includes racial or ethnic origin, trade union membership or political opinions.

'processing' of personal data means any operation performed on personal data and includes collecting, recording, holding or storing data and also adapting, altering, using, disclosing, transferring, deleting and destroying it.

Data Protection Principles under UK GDPR

Article 5 of the UK GDPR sets out six privacy principles. In summary these state that personal data shall be: -

1. processed lawfully, fairly and in a transparent manner.
2. only used for the specific purpose it has been collected for unless you have consent from the data subject to use it for something else.
3. collected in a way that means as a data controller you only process the minimum amount of personal data that is needed for your purposes.
4. accurate and, where necessary, kept up to date.
5. kept only for as long as it is needed for.
6. processed in a way that ensures there are appropriate security measures in place to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

What information do we process?

The University processes a number of different types of personal data to allow us to carry out our functions. For example, we process staff details so that we can administer our payroll systems. We also process information about our students and graduates so that we can administer fees, scholarships and bursaries for our students. There are also times when we process information about third parties such as our suppliers.

The University has a number of privacy notices that set out how we will process that various types of information we hold. For example, each year the University publishes a privacy statement that sets out in more detail how and why we process our students' data. We also have a similar privacy statement for staff so that employees are made aware of how we process their information when they start working for us. You can find a copy of our privacy notices on our webpage.

How are we ensuring we meet our legal requirements?

There are a number of ways we ensure we meet our legal requirements: -

Processes and procedures

We have appropriate procedures in place to make sure we meet the requirements under the legislation, for example, our data breach procedure which is explained later in this Code of Practice and our Data Handling and Classification Protocol.

Providing staff awareness training

We provide data protection training to all staff. Online training is made available to new staff when they join the University and to all existing staff training is refreshed every two years. Bespoke in-person training is also available to any Schools or departments who request it.

Implementing technical and organisational data security measures

The University must retain and build public confidence that personal data is held securely. The right level of protection varies significantly depending on the category of personal data held (e.g. if it is sensitive personal data). A risk assessment should be undertaken, in line with our Data Handling and Classification Protocol, to ensure the appropriate level of security is applied.

All staff are responsible for ensuring that any personal data they hold is kept secure and that it is not disclosed to any unauthorised third party.

Legal basis for its data processing activities

The University holds a register of our data processing activities as is required under the UK GDPR. This contains details of all personal data that we process and the reason why we process it. There is various legal basis on which the University can process personal data. We always make sure we are accountable for what we do with the information we should but having an appropriate legal basis for processing personal data before doing so. One of the basis is that we have a legitimate interest in doing so. Where we rely on our legitimate interest as the basis for processing data then we make sure that we have carried out a legitimate interest assessment, where this is required by the legislation.

Retention of Data

Personal data should only be kept for as long as is necessary to fulfil the purpose for which it was collected. The University has record retention schedules which set out how long personal data should be kept for. These are available on the University website. All staff should ensure that they comply with the records retention schedules in relation to personal data that they are responsible for.

International Transfer

The UK GDPR states that personal data should not be transferred outside of the European Economic Area (EEA) unless specific conditions are met. To make sure we comply with this the University makes an assessment before transferring data outside the EEA to make sure we are complying with the legislation, such as when we are transferring information to our Transnational Education (TNE) partner institutions.

If a member of staff is unsure whether a transfer of personal data outside of the EEA is permitted, then advice should be sought from the Legal Services team before any transfer takes place.

Data Sharing and Data Processing

The University collects a wide range of personal data relating to staff and students for its own purposes and to meet its external obligations. On occasions the University may share such data with third parties if we are allowed to under the legislation. Before doing this, we will make an assessment to ensure any data sharing is carried out lawfully.

Any member of University staff, who is considering an arrangement/agreement that involves sharing data, should consult with the Legal Services team before any data sharing takes place. Where it is decided that data sharing is permitted, a data sharing agreement must be put in place before any data transfer takes place.

There may be occasions where the University appoints a data processor for specific projects or processes. The UK GDPR outlines specific contractual requirements that must be in place before any data processing can start. If a staff member becomes aware that data is to be passed to a third party to process on our behalf, then the Legal Services team must be informed before any transfer takes place.

Privacy Impact Assessments (PIA)

When considering adopting new administration systems and other processes with possible privacy implications or updating existing systems or processes (such as student information system, virtual learning environments, distance learning programmes), University staff should undertake a Privacy Impact Assessment (PIA) in the early stages of the project or design process.

Responsibilities

The Court of the University of the West of Scotland is a data controller under the UK GDPR and has a corporate responsibility for implementing the provisions of the legislation and committing the organisation to providing the necessary resources to ensure that compliance is achieved. The Legal Services team is responsible for day to day data protection matters, the development of guidance and training for staff and the processing of Subject Access Requests.

The Head of Legal Services is the appointed Data Protection Officer for the University. If you have any concerns about how we handle your personal data then you can contact the Data Protection Officer directly by e-mail dataprotection@uws.ac.uk or by post at Data Protection Officer, University of the West of Scotland, Legal Services, High Street, Paisley, PA1 2BE. All staff have a responsibility to ensure compliance with the UK GDPR principles noted above and this Code of Practice. If there is uncertainty about the appropriate action to take when processing personal data, advice must be sought from the Legal Services team.

Staff responsible for supervising students undertaking work that involves the processing of personal data must ensure that students are given appropriate guidance to ensure compliance with this Code of Practice and the legislation and are aware of the consequences of not adhering to this.

Other Matters

Display or Publication of Personal Data

It is University practice that names, work telephone extension numbers, and email addresses of members of staff are published on the University's website, where these facilitate the normal organisational functioning and management of the University. Any staff member, with good reason, wishing to be excluded from these listings, should contact their Dean of School/Head of Professional Service.

Schools may display personal data relating to students, such as name and student ID number on notice boards and the intranet to provide information about seminar or tutorial groups, class tests and other essential information that has to be communicated. If a student objects to personal data being displayed in this manner, it is their responsibility to contact the School.

Access to Data

Individuals may request access to their own personal data held by the University via a Subject Access Request. To facilitate access to personal data the University encourages staff to make an informal request, in the first instance, to People and Wellbeing and current students to Registry, setting out details of the information required.

Where an individual considers that further information is required, they should be asked to submit a formal subject access request to the Legal Services team. Further information is available on subject access requests on the data protection section of the University's website.

Complaints Process

In line with the University values, we hold ourselves accountable for how we use personal data. We have a complaints process on our website which tells people how they can make a complaint to us and we will use the outcome of the complaints to make sure we are accountable for any mistakes we make and take action to make sure it does not happen again.

Email and Internet Use

The University reserves the right to monitor use of email and internet facilities in compliance with current legislation.

Data Breaches

A data security breach is considered to be any loss of, or unauthorised access to, data belonging to the University (normally involving personal or confidential information). Examples of this include loss or theft of equipment (such as mobile phones or a laptop) loss of paper records or personal data being e-mailed to an incorrect recipient.

Breaches such as those mentioned above can damage the University's reputation and its relationship with its stakeholders. It also exposes the University, its staff or students to the risk of fraud or identity theft and can cause considerable distress to those concerned.

The University needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure we can act responsibly, protect our information assets and are accountable when things go wrong. The aim of such a process is to standardise our response to any reported data breach incident and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

Our data breach procedure can be found at Annex 1. All staff are required to follow this procedure in the event they become aware of a data breach.

CCTV
The University has in place a comprehensive closed-circuit television (CCTV) surveillance system across its campuses. The main purpose of this system is to reduce crime, but additional benefits include the provision of a safe and secure environment for students, staff and visitors, and the prevention of the loss of, or damage to, University property.

Body-worn cameras may be used by our security staff. Security staff members will activate cameras where there is a recognised requirement to record footage and will let individuals know that video and audio recording will take place. Images captured by body worn cameras will be treated the same way as CCTV footage for the purposes of this Code of Practice.

The CCTV system records and processes images of identifiable individuals, which constitutes personal data under the UK GDPR. Therefore, the University must ensure that our use of CCTV systems complies fully with the legislation and the most recent CCTV Code of Practice published by the Office of the UK Information Commissioner (ICO). Further information can be found at Annex 2.

Photography and Filming
Images of individuals, whether contained in a photograph or in filmed footage, will often be caught by the definition of personal data under the UK GDPR. Guidelines are available for staff to follow should they wish to film or photograph individuals for University purposes. They can be found on the Legal Services page of the intranet.

Generative Artificial Intelligence (GenAI)
The University has guidance on the use of personal data and other information with Generative Artificial Intelligence (GenAI), further information can be found under Annex 3 with a link to the guidance document - Academic Integrity and Artificial Intelligence Staff Guidance.

Real Data Testing
Guidance is provided on using personal or real-world data for testing and training under Annex 4.

Legal Services Contact Details
If there are any questions about this Code of Practice you should contact the Legal Services team at dataprotection@uws.ac.uk

.

Annex 1 – Data Breach Procedure

If a staff member becomes aware of a data breach, or suspected data breach taking place then they must report this to their line manager in the first instance. Line Managers are requested to report matters as soon as possible to the Legal Services team using the Data Breach Reporting Form. If the matter is urgent and needs immediate attention, then reports can be made to the Legal Services team on dataprotection@uws.ac.uk and the form can be completed once the immediate actions have been dealt with.

If the breach occurs due to the loss or theft of mobile devices, IT should also be informed so that, where possible, action can be taken to secure any information held on the device.

After a breach has been reported the Legal Services team will support the reporting School or department in implementing the appropriate steps for breach management.

Containment and Recovery

If the reported breach is not serious, the Legal Services team, in consultation with the Line Manager in the area responsible for the breach will determine what action to take and who needs to be aware of the breach. If the breach is classed as 'serious', the Vice Principal (Governance) and University Secretary will be informed. The UK Information Commissioner does not define the term "serious breach" but the overriding consideration is determining the potential detriment to data subjects, and the volume and sensitivity of personal data lost / released / corrupted. The Vice Principal (Governance) and University Secretary will appoint a member of staff to lead the investigation into any serious breaches, ensuring that adequate resources are assigned to this task.

The investigation must establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. Also, it must establish whether there is anything to be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back-up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

Assessment of the ongoing risk

Before deciding on what steps to take to contain the breach, the potential adverse consequences for the individuals whose data was compromised must be assessed by the Legal Services team and the owner of the data. The following should be taken into account:

- The type of data involved.
- The sensitivity of the date.
- If data has been lost or stolen, are there protections in place such as passwords or encryption?
- What has happened to the data? Has it been stolen or damaged or lost? Has it been disclosed in error or to the wrong recipient?
- What could the data tell a third party about the individual?

- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Is there a risk to public health or loss of public confidence in an important service that we provide?

Notification of the Breach

An important element in managing a breach is informing the individuals or organisation whose data has been compromised and being accountable when a breach has occurred. Notification will enable individuals affected by the breach to take steps to mitigate the risks and to allow the appropriate regulatory bodies to provide advice, deal with complaints and perform their functions. In deliberating the most appropriate way to notify those affected, the urgency of the situation and the security of the medium are key considerations. Notification should include:

- A description of the data involved.
- Details of how and when the breach occurred.
- What action has already been taken to respond to the risks posed by the breach.
- Specific and clear advice on the steps that an individual can take to protect themselves and what the University is willing to do to help them; and
- Contact information e.g. helpline, webpage

Consideration should be given to notifying third parties such as the police, insurers, bank or credit card companies, and the trade unions.

The Legal Services Team will be responsible for making any report to the ICO, where the breach meets the legal threshold for reporting.

If the press is aware of the loss or breach, working with the UK Information Commissioner helps to minimise the damage to an organisation's reputation.

Marketing should be consulted about issuing a press release if it is clearly in the interests of the individuals whose data has been compromised, or there is a strong public interest argument to do so.

Evaluation and Response

When a breach occurs, it is important to investigate not only the causes of the breach but the University's response to it in case there are systemic or ongoing problems. For example, if there was a lack of clear allocation of responsibility or inadequate policies or procedures. Monitoring of staff awareness of security issues may reveal gaps that can be filled through tailored advice or training. Risks will arise when sharing data with or disclosing data to others. The storing or transmission of personal data on portable or mobile devices is a weak point in security measures if encryption is not employed.

Details of all breaches will be recorded by the Legal Services team in the log of Data Protection breaches. Where the breach is serious, a written report may also be prepared for the Vice Principal (Governance) and University Secretary after the investigation is complete and mitigating action taken. Any disciplinary action resulting from the investigation will fall under the normal agreed disciplinary procedures.

Annex 2 - CCTV

Our system

Currently CCTV cameras are located in publicly accessible space and teaching areas on all campuses. In addition, seven laboratories, a server room and the entrances to a music room and games room in the School of Computing, Engineering and Physical Science on the Paisley campus have CCTV equipment. There is no CCTV equipment in any private rooms or staff rooms except in the staff area of the Student Hub on Paisley campus.

The images from the CCTV system are monitored in control rooms at each campus. The campuses at Paisley and Ayr are staffed by University Security staff. At night and during weekends suitably qualified suppliers, holding a Security Industry Authority (SIA) licence, replace University Security staff at Paisley Storie Street Residence and Ayr campus.

How we ensure compliance with the legislation?

The University takes various steps to ensure our use of CCTV is compliant with the legislation. This includes: -

1. Conducting privacy impact assessments prior to the installation of new CCTV equipment to ensure any use is appropriate, proportionate, transparent, and effective in meeting its stated purpose.
2. Locating cameras at strategic points on campus, principally at the entrance and exit point of sites and buildings, communal areas within residences and some engineering laboratories and ensuring that no cameras are hidden from view or focus on the frontages or rear areas of private accommodation.
3. Placing signs prominently at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV installation is in use.
4. Ensuring systems will not be used to provide recorded images for the internet, to record sound or for any automated decision taking.

In addition, when operating the systems the following procedures are in place: -

All security control rooms for monitoring images are self-contained with limited access. The rooms have monitoring equipment to allow security officers to monitor live images from the cameras, but screens are not visible from outside of the control room/area.

Access to the control rooms is limited to those who have sufficient and justified reason to have access (e.g. official visits from law enforcement, cleaning staff, security staff and senior management) and only then with the personal authority of the Head of Campus Services. (All persons visiting the control room with the purpose of viewing recorded data will be required to sign the visitors' book. Other personnel, such as cleaning staff or engineers effecting repairs, must be authorised by the Head of Campus Services and will be supervised at all times.

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV images and recordings and will be provided with appropriate training.

Any misuse of information obtained from a recording will be considered a serious disciplinary offence and will be dealt with accordingly.

The Control Rooms are supported by a digital recording system which stores images on a University server. In accordance with the fifth principle in the UK General Data Protection Regulation recorded material will not be kept for longer than is necessary. Recordings will be retained for a calendar month before being overwritten or erased unless a request for access has been intimated.

Images from the School of Computing, Engineering and Physical Science cameras are viewed only by the Network Support Analyst. Images from the School of Computing, Engineering and Physical Science cameras are held on a personal computer for one week.

Access and Disclosure of Images

Access to and disclosure of images captured by our CCTV system is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Where an individual wishes to access a copy of a CCTV recording, they may do so by contacting the Legal Services team (dataprotection@uws.ac.uk) who will handle the request in line with our Subject Access Request procedures.

Where a request is received from a third party, for example, in relation to the investigation of a crime, then such third parties are required to show adequate grounds for disclosure of images and must be accompanied by written authority under which the request is made and reasonable proof or organisational affiliation. Any such requests will be assessed on a case-by-case basis by the Legal Services team in association with the appropriate staff member, e.g. Operations Manager (Estates). Access will only be granted where it is consistent with the obligations placed on the University by the legislation. Disclosure to a representative of the Police is not compulsory except in cases where the University is served with a court order.

Responsibility for the System

The Head of Campus Services is responsible for the physical security of staff, students, buildings and contents on campus and the residencies. The Head of Campus Services has the responsibility to investigate where the use of CCTV is not in line with this procedure. The Dean of the School of Computing, Engineering and Physical Science will investigate if the concerns relate to use of the system in the School of Computing, Engineering and Physical Science. The Head of Campus Services has delegated day-to-day responsibility for the CCTV system to the Security Services Manager. The Network Support Analyst has day-to-day responsibility in the School of Computing, Engineering and Physical Science.

If use of the CCTV system is in breach of the legislation, then the Head of Legal Services must be informed and procedures laid down for data breaches will be followed.

Where staff, students or visitors to the University have concerns or complaints about the operation of the system, this should be addressed, in the first instance, to the

Security Services Manager, the Head of Campus Services or the Dean of the School of Computing, Engineering and Physical Science, as appropriate. If the concerns or enquiries relates to a breach under the legislation these may be addressed to the Legal Services team at dataprotection@uws.ac.uk.

Annex 3 – Procedure on the use of personal data and other information with Generative Artificial Intelligence (GenAI)

Introduction

Generative AI is a broad term used to describe any type of artificial intelligence (AI) that can be used to create new text, images, video, audio, or code.

ChatGPT is an example of a publicly available, web-based version of generative AI. This produces text outputs on a particular subject based on previously inputted/uploaded material. The tools can be used to summarise articles/reports, or to generate answers to a question, or to produce code.

Although it is recognised that the use of AI technology may have benefits to the University, we must make sure that when using these we have an awareness of the risks and take appropriate action to mitigate against these.

Purpose and scope

These guidelines set out how University staff, contractors and students are permitted to use generative AI tools when carrying out University business to ensure that we meet our obligations under data protection law.

The University has developed separate guidance and resources on the use of Generative AI in the teaching, learning, assessment.

Restrictions on Use of AI

1. Any information classified as Restricted or Confidential must not be submitted to generative AI tools (such as ChatGPT). Detail on what Information falls into these classifications can be found within our Data Handling and Classification Protocol.

   This includes the personal data of our staff, students, visitors, research participants and others and also sensitive non personal information that is commercially sensitive data.

2. Information that, if compromised or lost, could have damaging consequences for other individuals, groups of individuals, or the University more generally (including reputational damage) should not be submitted into generative AI tools, for example copyright protected materials, where the volume of material exceeds the provisions for fair dealing, available to educational institutions and students.
3. University passwords and usernames should never be inputted into AI tool.
4. Any data related to University Intellectual Property.
5. Any non-personal data from third parties where the individual has not explicitly consented for their data to be used with AI, with the exception of data that is clearly already in the public domain.

Use of ‘approved’ Generative AI tools

The use of any new AI tools involving the categories of restricted data set out above must be requested via logging a change request with the IT service desk (helpdesk@uws.ac.uk). IT will maintain a register of University approved Generative AI tools, outlining what levels of data and information can safely be used within those applications, and for what purposes.

The selection and procurement of generative AI tools should follow existing University policies and procedures for the procurement of goods and services.

Before personal data which the University is responsible for is used in approved generative AI tools, it will necessary to first contact a Data Protection Impact Assessment ("DPIA").
This will allow the privacy risks to be identified, lower risk alternatives to be identified and appropriate mitigations to be implemented. Please liaise with the University Data Protection Officer for help (dataprotection@uws.ac.uk)

Should the University make available access to enterprise or organisational licensed AI tools, it is the expectation that these will be used as opposed to individual accounts. Co-pilot is the currently supported University AI tool and is available with a UWS Microsoft licence.

Requests for use of other tools will only be approved in exceptional circumstances where a suitable business case is shown.

Contacts and further information

The University has a legal obligation to keep personal data secure and to investigate any suspected breaches. If a member of University staff becomes aware of any generative AI tool use that is not in line with the rules set out in these guidelines this should be reported to the data protection team by e-mailing dataprotection@uws.ac.uk.

Any questions on the use of such technologies should be directed to IT service desk (helpdesk@uws.ac.uk) in the first instance, with questions on the use of personal data directed to the Data Protection Officer (dataprotection@uws.ac.uk)

Questions on the use of this technology in teaching, learning and assessment should be directed to learning.transformation@uws.ac.uk.

Annex 4 – Real-World Data Testing

Guidance on using personal or real-world data for testing and training

1. Introduction

1.1. The Information Commissioner's Office (the "ICO") strongly recommends that personal data is not used for the development and testing of software and/or systems. This is because during development and testing it is expected that failures will occur and as a result of this data may be exposed, leading to harm.

1.2. Anonymous data should be used instead of personal or real-world data wherever possible in the development and testing of software and/or systems. In support of this recommendation the ICO provides additional guidance on anonymisation.

1.3. However, it is recognised that there will be some cases where personal or real-world data to deliver effective testing and/or training. In these cases, the use must not compromise an individual's right to privacy and our legal obligations, which include maintaining the security of personal data.

2. Definitions

2.1. The following definitions apply to this guidance:

- **Personal or real-world data** refers to data collected or created by the University that is linked or can readily be linked to a person, for example, staff salary information or student exam results.
- **Anonymised data** means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in a way that the data subject is not or no longer identifiable'.
- **Pseudonymisation** is 'the process of distinguishing individuals in a dataset by using a unique identifier, held by the University which does not reveal their 'real world' identity'

3. Principles

3.1 Only anonymised data for system and/or application development, testing and training should be used unless necessity has determined otherwise and written approval has been granted in line with this guidance.

Where approval is requested an appropriate risk assessment and due diligence must determine that it is necessary to use personal or real-world data for development, testing or training activities and that use of those data can be made safely and securely then such data may be used under the stated conditions. Necessity will be determined by application of the following questions:

3.1.1 Is it possible to make use of **replacement alternatives**, i.e., anonymised or pseudonymised data for a given development, testing or training activity? If yes, then personal or real-world data cannot be used as a safer alternative is available.

3.1.2 To what extent can the use of **reduction alternatives** be made, i.e., if personal or real-world data are to be used how do we use the minimum set in terms of volume and sensitivity for a given development, testing or training activity?

3.1.3 How do we **refine** the period of a given development, testing or training activity so that we use personal or real-world data only for the shortest

necessary time to reduce risk?

3.2 Where the University has determined the use is necessary then only the use of minimum personal or real-world data may be approved in terms of volume, sensitivity and the time limit for use.

3.3 Where it is necessary for data to persist for more than a minimum period in non-production environments for the general purposes of system and/or application development or training, and anonymisation is not feasible, then the University will use pseudonymised data, i.e., synthetic or other alternative data values will be substituted for personal or real-world data.

3.4 Training materials, e.g. handouts, guidance documents, whether secured online or not, will only use anonymised data. The use of personal or real-world data in training materials is not permitted.

4 What data can't be used for testing?

In addition to Restricted and Confidential data, the following data items are never permitted to be used for testing purposes:

- real world email addresses (excluding those of the users testing)
- national identifiers, e.g. NI number, passport number
- Student applicant/application data during the UCAS embargo periods (as defined by the University)

The presumption is that real world data will not be permitted for use in the early stages of testing when it is more likely for the trial to go wrong.

At the same time the presumption is that you will be permitted to use real world data if:

- you are using fully anonymised data
- you already have approval to use such data repeatedly throughout project development
- you are using a synthetic or other pre-approved dataset for testing or training purposes

5 Process

It is recommended that a testing or training schedule/plan is developed early in the project/work lifecycle, to identify at the earliest opportunity requirements where use of personal or real-world data may be necessary and, consequently, the preparation of a request can be factored into the project plan.

In some cases, a Data Protection Impact Assessment ("DPIA") must be undertaken at the same time.

Colleagues who believe an exception is necessary to enable their use of personal or real-world data for the purposes of system and/or application development, testing or training must make a written case in advance as outlined in the above guidance. Submissions should be made to data.protection@uws.ac.uk using the template at Annex 4a.

Submissions requesting the use of personal or real-world data for system and/or application development, testing or training will be considered on a case-by-case basis and reviewed in light of the above principles and protocol.

The Data Protection Officer (Legal) and IT Security Manager (IT) will be responsible for reviewing any requests and will make a decision on a case-by-case basis.

Annex 4a - Request to use real-world data for testing or training purposes

Question	Response
Does the request build on a previously submitted request? If so, please provide details	
Have you previously used the dataset for testing or training without risk?	
Type of data to be used (including whether it contains personal information):	
Location of real-world data (i.e., where is the data currently held):	
Proposed new location of real-world data (i.e., where is the test data to be held):	
Quantity / volume of data requested (i.e., how many discrete individuals will be in the dataset):	
Who is the data owner?	
How often and how long will the data be used for testing or training:	
Estimated start date for use of the data for testing or training:	
Description of Test Environment: - • Where is the test environment? • Is the test environment new or one that has been used for similar activities? • Can anyone hack into the environment? or can data escape the environment into a real-world process such that an individual or the institution is harmed? • How secure is the test environment? How has this been evaluated?	
Purpose of testing • What is the objective of testing, i.e., what are you demonstrating or looking to see fail in your testing? • Have you run any tests with anonymised data for this	

same process? • Will you be running multiple tests in the same environment?	
Test outcomes • What is your testing or development objectives?	
User access • Who will have access to the test data. • How will users be controlled? • What is the minimum number of users required for a successful outcome?	
Data migration • How will data be migrated from the production to the test environment? • If the data are being downloaded and then imported describe how the downloaded data will be controlled and deleted after import. • Will the data be migrated once? Or iteratively?	
Data ownership • Have you consulted the data owner(s) and familiarised them with the proposal?	
Risk analysis • What risk is there if the test environment were compromised/hacked? • Could the data be accidentally used in the test environment in a way that would result in a real world detriment (e.g., a user thinking the data in the test environment is in fact real live data)? • How long will the data persist in the environment? • Is there any foreseeable reputational risk to the University? • What steps have you taken to ensure that the length of time has been **refined** so it is of the shortest period to reduce risk?	

Submitted by:-

Date:-