DATA PROTECTION CODE OF PRACTICE

1. INTRODUCTION

The University is committed to the principles and obligations set out in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). We handle a large amount of personal data, and we take our responsibilities for data privacy seriously.

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 GDPR which requires the University, as a data controller, must 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

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 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 GDPR

Article 5 of the 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 where we process information about third parties such as our suppliers.

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.

How are we ensuring we meet our legal requirements?

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

A - 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 Protocol on the use of cloud storage.

B - 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 on an annual basis. Bespoke in-person training is also available to any Schools or departments who request it.

C - 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, 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.

D - Legal basis for its data processing activities

The University holds a register of our data processing activities as is required under the GDPR. This contains details of all personal data that we process and the reason why we process it. There are various legal basis on which the University can process personal data. We always make sure we have 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.

E - 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 Legal Services intranet page. All staff should ensure that they comply with the records retention schedules in relation to personal data that they are responsible for.

F - International Transfer

The 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.

G - 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 controller for specific projects or processes. The 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.

H - 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, ePortfolio systems), University staff should undertake a Privacy Impact Assessment (PIA) in the early stages of the project or design process. Further advice is available from the Legal Services Intranet page.

RESPONSIBILITIES

The Court of the University of the West of Scotland is a data controller under the 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 University Solicitor 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 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 Organisational Development, and current students to Student Administration, 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. Details about the process can be found here.

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 expose 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 and protect our information assets. 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.

The CCTV system records and processes images of identifiable individuals, which constitutes personal data under the 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 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.

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 by telephone to the Legal Services team on 0141 848 3699.

If the breach occurs due to the loss or theft of mobile devices, ITDS 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 Director of Corporate Support 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 Director of Corporate Support 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 whose data has been compromised and any relevant organisations. 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 ICO believes that serious breaches should be brought to his attention though, at present, there is no law expressly requiring universities to provide notification of a breach. 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. Any notification on behalf of the University will be made by the Legal Services team.

Corporate 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 Director of Corporate Support 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, six laboratories and a server room in the School of Engineering and Computing 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 and Facility Management Operatives (FMOs). Hamilton employs an independent security contractor. At night and during weekends suitably qualified contractors, 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 Commercial Services (residences) or the Head of Estates Management (non-residential). All persons visiting the control room with the purpose of viewing recorded data will be required to sign the visitors' book and a declaration of confidentiality. Other personnel, such as cleaning staff or engineers effecting repairs, must be authorised by the Head of Commercial Services or the Head of Estates Management (as appropriate) 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 principal in the Data Protection Act 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 Engineering and Computing cameras are viewed only by the Engineering Systems Manager. Images from the School of Engineering and Computing 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. Facilities Manager. 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 Estates Management is responsible for the physical security of staff, students, buildings and contents on campus, except for the residencies, which are the responsibility of the Head of Commercial Services. Both posts have the responsibility to investigate where the use of CCTV is not in line with this procedure. The Dean of the School of Engineering and Computing will investigate if the concerns relate to use of the system in the School of Engineering and Computing. The Head of Estates Management has delegated day to day responsibility for the CCTV system to the Facilities Manager at each campus. The Engineering Systems Manager has day to day responsibility in the School of Engineering and Computing.

If use of the CCTV system is in breach of the legislation, then the University Solicitor 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 Facilities Manager, the Head of Commercial Services or the Dean of the School of Engineering and Computing, 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.