# Data Protection Policy

## 1. Introduction

USW Commercial Services Ltd ("**USWCS**") is a wholly owned subsidiary of the University of South Wales (the "**University**") and takes the protection of all personal data seriously and is fully committed to the protection of the rights and freedoms of all individuals in relation to the processing of their personal data. Personal data will be processed in compliance with data protection laws.

This policy is supplemented by guidance documents, which must also be adhered to as part of this policy. A glossary of terms is included as Appendix 1.

## 2. Purpose

To undertake its core functions and other services it is necessary for USWCS to collect, store and use personal data of clients and their employees. This policy details the standards that USWCS will follow and provides clarity for individuals, clients and client employees on the expectations of USWCS when personal data is processed.

## 3. Scope

This policy applies to all University employees working with USWCS, including, temporary, casual, contract, volunteers, agency staff and external consultants, as well as any processors acting on behalf of USWCS (the **"Individuals**").

This policy should be read and interpreted, in conjunction with, the USWCS handbook, consultancy agreement and any other related USWCS and University policies and published guidance.

## 4. Responsibilities

USWCS is the 'data controller', and will respond appropriately to ensure data is processed compliantly and protects data subject's rights under the Regulations.

USWCS is legally required to have in place a Data Protection Officer (DPO) who is responsible for areas including; the management of: day-to-day data protection matters, training, developing good information handling practice across USWCS, monitoring compliance and advising the necessity of data protection impact assessments.

USWCS Directors are responsible for overseeing compliance with this policy and ensuring good data protection practice within USWCS. USWCS will designate a Data Coordinator whose role will be to cascade information into management team meetings and identify new processing activities that involve personal data.

All Individuals are responsible for ensuring that they adhere to data protection laws and policies when processing personal data. They are also responsible for ensuring that any changes to personal data that USWCS holds is accurate and up-to-date by informing USWCS of any changes or errors immediately.

## 5. Data Protection Principles and Individual Rights

When processing personal data, USWCS is committed to complying with data protection laws. Personal data will be processed in accordance with the 6 Principles of the General Data Protection Regulation (GDPR):

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

USWCS will ensure that personal data will be processed in line with the rights of the individual:

- **The right to be informed** – Individuals will be advised how their personal data is used.
- **The right of access** – Individuals will have a right, upon request, to obtain a copy of their data.
- **The right to rectification** – Where appropriate, individuals are entitled to have inaccurate data rectified.
- **The right to erasure** – Individuals are able to request that personal data is erased.
- **The right to restrict processing** – Individuals may suppress processing where appropriate.
- **The right to data portability** – Individuals may request their information be moved from one IT environment to another without hindrance to usability.
- **The right to object** – Individuals are able to object to processing in prescribed situations.

- **Rights in relation to automated decision making and profiling** – where decision-making is made automatically, individuals can object to their data being processed in this manner.

## 6. Processing personal data lawfully and fairly

USWCS collects personal data in the provision of services to service users together with other purposes relating to its functions.

To ensure that personal data is processed fairly, there is a requirement to ensure that clients are made aware of how USWCS will use their data. To ensure compliance:

- Clients will be directed to our fair processing notice/privacy notice when their personal data is collected.

- Where personal data is obtained from other sources, USWCS will provide the client with information relating to the processing within one month of obtaining the data.

For personal information to be processed, there must be a lawful basis for the processing. When special category personal data is processed, additional conditions must be met.

## 7. Security of personal data

USWCS and the Individuals will ensure that it manages personal data, held in electronic and hard copy securely. The Individuals must comply with University IT Security Policies, and Information Handling Policies and Guidance when handling personal data.

All Individuals (where informed by USWCS) who will be handling personal data are required to complete the University's Mandatory Data Protection and Information Security training.

Where applicable training must be completed within 2 weeks of the projects commencement at the latest. Thereafter, all Individuals handling personal data are required to complete the University's mandatory refresher training at least every 2 years.

Failure to complete the mandatory training (if applicable) within the timeframes set would constitute a breach of this policy and may result in action being taken against the Individual.

USWCS will maintain a record of all Individuals who have completed and passed the training in order that it can demonstrate compliance with its data protection obligations. Where an Individual fails to complete the training within the specified time a notification will be sent to them.

Where Individuals are working with partners/other organisations, which involves the processing of personal data, there is a requirement on USWCS to ensure that respective responsibilities on both parties are included in a contract.

In the event that USWCS engages a third party as a 'data processor' for its personal data, a specific written contract with the third party providing assurance in respect

of the management of the data must be in place.

A data security breach involves the loss of, or unauthorized access to, personal or confidential data including information in hard copy and electronic format and could include – theft or loss of data, accidental disclosure and malicious access to data or intellectual property. This includes both information in hard copy and electronic information. Where a breach occurs Individuals must report the incident in line with the Data Breach Procedure within 12 hours of becoming aware of the breach.

When processing personal data Individuals will do so in accordance with the Information Classification Policy.

Where Individuals are considering using a new system to store, collect or process personal information the Individual must inform USWCS who will consult with IT and a security assessment must be completed

Offices or rooms containing personal data must be locked when empty or not in use and desks, cupboards and filing cabinets must be kept locked if they contain personal or confidential data.

When Individuals vacate rooms or close IT systems they must ensure that steps are taken to protect personal data and to ensure that it is kept in a way that is accessible to others and kept in line with the University retention policy.

Paper documents containing personal data must be disposed of securely via the University's confidential waste service or confirmed as destroyed upon request. Electronic data or media such as USB sticks, CDs must be wiped or destroyed securely to ensure that the information is no longer accessible. Equipment such as laptops, PCs, smartphones must be wiped and/or disposed of securely.

Monitors must be positioned in locations that ensure confidential information is not visible to passers-by or other unauthorized individuals e.g. through office windows or doors. Users must lock their PCs and other devices when they are left unattended to prevent unauthorised access to systems.

Paper records containing personal data must be kept securely to prevent unauthorised disclosure. When not required, the paper or files should be kept in a locked drawer or filing cabinet.

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

USWCS will undertake a Data Protection Impact Assessment when using new technology that involves the processing of personal data, or, where the processing is likely to result in a high risk to the rights and freedoms of individuals.

Individuals must only process personal data belonging to USWCS when there are lawful grounds to do so and when they are authorised to process that data. Unauthorised processing of personal data includes (but is not limited to) accessing personal data for private interest or personal gain. In addition to being a disciplinary

offence, accessing personal information can be a criminal offence for which individuals can be prosecuted.

Individuals will not disclose information to (for example but not limited to) third parties such as employers, sponsors, the police unless there is a legal basis or an exemption that allows them to provide the information.

Personal data must not be transferred to a country outside the EEA (European Economic Area) unless that country has adequate measures in place to ensure that the rights and freedoms of data subjects are protected when their personal data is processed.

## 8. Management of records

Personal data held about individuals must be sufficient for the purposes for which it is held. The minimum amount of personal data needed will be identified and collected; additional, excessive personal data must not be held.

USWCS will ensure that personal data is accurate and where necessary, kept up-to-date. The accuracy of personal data will be checked regularly and data subjects should have a means of updating their information when required.

USWCS will only keep personal data for as long as is necessary in accordance with a legal requirement and retention schedules maintained by USWCS. Information identified for destruction will be erased or disposed of securely.

Personal data will only be processed for the specific purposes notified to the data subject via the privacy/fair processing notice when the data was first collected or for any other purposes specifically permitted under data protection legislation. Personal data must not be collected for one purpose and then used for an entirely different, unrelated purpose. Where it is necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs, unless an exemption from this requirement applies.

## 9. Governance and accountability

USWCS will appoint a Data Protection Officer (DPO) who will report to the Vice-Chancellor of the University and a regular report will be presented to a formal meeting of the University's Information Security Board.

Individuals or clients wishing to make a complaint may do so through the 'USWCS Complaints Procedure'.

## 10. Consequences of non-compliance

It is a condition of employment in the case of staff/contractors/agency workers and contract/terms & conditions of engagement for consultants, that they will abide by the policies and rules of USWCS and where applicable the University.

Any breach of this policy is considered a breach of contract and USWCS will take further action. A serious breach of the Data Protection Regulation may result in USWCS being liable in law. In certain situations, Individuals can be personally prosecuted for breaches of the data protection law.

**Appendix A**

The General Data Protection Regulation governs the processing of personal data. All these terms are defined in the Regulations.

**Personal data** means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particularly reference to an identifier such as name, id number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

**Special Category/Sensitive personal data is** personal data relating to ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures.

A **Data Subject** is the individual who is the subject of personal data.

**Processing** means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as 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

A **Data Controller** means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

A **Data Processor** means a natural or legal person, public authority, agency or any other body, which processes personal data on behalf of the controller.

# Rights of the Individual under the GDPR

The General Data Protection Regulations provides additional rights and strengthens rights to individuals in respect of how personal data is processed.

Individuals have the following rights:

- The right of access
- 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 processing

Further advice and guidance is available from the University's Information Compliance Manager (dataprotection@southwales.ac.uk)

**The right of access**

Individuals have the right to obtain confirmation from USWCS around whether their personal data is being processed and for access to their data including information about:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom data will be disclosed.
- Retention of the data.
- The existence of the right to request rectification, erasure or restriction of the processing of personal data.
- The right to lodge a complaint to the Information Commissioner's Office.
- Where the data has been collected from when the personal data has been collected from sources other than the individual.
- The existence of any automated decision making relating to their personal data.

To make a request, individuals may submit a request through the following **link** and by completing the appropriate fields.

Upon receiving the request, the University will confirm receipt of the request and will require the individual to provide identification documentation to the University in order that it can verify and confirm the identity.

The University will request information that will enable it to identify which members of staff need to be contacted to obtain this information.

The University may contact individuals seeking their information if there is a need clarification on the scope of the request.

In accordance with the GDPR the University may, if a request is manifestly unfounded or excessive, charge a reasonable fee or refuse to respond.

The Information Compliance Manager will contact those members of staff identified requesting that they provide the data held. Information returned by employees will be reviewed by the Information Compliance Manager who will ensure that data which the individual is not entitled to receive is removed.

The University will respond within one month of receipt of the request being received. In certain circumstances, it may be necessary for the University to ask for an extension of up to 2 months. Where an extension is sought, an explanation behind the need for additional time will be provided.

**The right to rectification**

If personal data is identified as inaccurate or incomplete, individuals have the right for it to be rectified within one month. Where the information has been shared with third parties there is a need to ensure that the third parties are also informed so that they can make rectifications.

To exercise their right to rectification individuals may submit a request through the following **link** and by completing the appropriate fields.

**The right to erasure**

Also known as the right to be forgotten; an individual has the right to have personal data removed or deleted within one month if there is no compelling reason for it being processed.

This right only applies in the following situations:

- When the data is no longer needed for the reason it was originally collected.
- The individual withdraws consent.
- The individual objects to processing and there is no continued legitimate reason to continue processing.
- The processing is unlawful – that is to process the data was in breach of the GDPR
- There is a requirement to erase the data to comply with a legal obligation.
- It is processed in relation to offer or information society services to children.

The University can refuse to comply with a request for data to be erased where personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information.
- In order to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes which are in the public interest.
- To archive in the public interest; scientific, historical and statistical research purposes
- To defend a legal claim.

To exercise their right to erasure individuals may submit a request through the following **link** and by completing the appropriate fields.

**The right to restrict processing**

Individuals have the right to block or restrict processing, which means that the University is able to store or hold personal data but not process it further.

This applies in the following situations:

- An individual contests the accuracy of the data, until the accuracy is confirmed.
- Where the individual has contested the processing and the University is considering if its legitimate interests override this.
- When the processing is illegal.
- If the University no longer requires the personal data, but the individual needs it to defend a legal claim.

If processing is to be restricted and it has been disclosed to a third party, it is necessary to advise the third party of this unless it would cause disproportionate effort to do so. If it is decided that the decision to restrict is to be lifted it will be necessary to advise the individual (data subject) that the restriction has been removed.

To exercise their right to restrict processing individuals may submit a request through the following **link** and by completing the appropriate fields.

**The right to data portability**

This allows individuals to obtain and reuse (i.e. move, copy and transfer) their information across different services for their own purposes.

This must be completed within one month of the request being made and a fee cannot be charged. This only applies to data provided by the individual, where the processing is carried out by automated means and the University has relied upon the individual's consent or for the performance of a contract as the legal basis for processing.

The personal data must be provided in a structured and commonly used form that will enable other organisations to use this data. When a request is received, if possible, the data must be transferred directly to the other organisation.

**The right to object**

Individuals have the right to make objections to the University around processing in the following situations:

- Where it is based on legitimate interests or the performance of a task in the public interest or the exercise of official authority.
- That relate to direct marketing (there are no exemptions).
- Processing for purposes of scientific/historical and statistical research purposes.

The University will stop processing unless it is able to demonstrate compelling legitimate grounds for the processing; or the processing is for the establishment, exercise or defence of legal claims.

Where an objection to direct marketing is received, the University will cease processing data immediately.

To exercise their right to object individuals may submit a request through the following **link** and by completing the appropriate fields.

**Rights in relation to automated decision making and profiling**

Safeguards exist within the GDPR where significant decisions or those that have a legal effect are taken by automatic means without human intervention.

Individuals have a right to get human intervention, give their own view, have the decision explained to them, and challenge that decision if they are not happy with it. This will not apply where the decision is:

- Necessary for entering into/the performance of a contract between the University and the individual.
- Authorised by law.
- Based on explicit consent.

With regard to profiling, this would include any processing used to judge an individual's; performance at work/study, economic situation, health, personal preferences, reliability, behaviour, location or movements. To undertake this type of processing requires precautions including appropriate Privacy Notices, statistical procedures and information security processes, as well as robust procedures to prevent errors.

# DATA BREACH PROCEDURE FOR INDIVIDUALS

## Introduction

Personal data breaches can cause real harm and distress to individuals and can provide the opportunity for identity fraud. How USWCS handles such an incident will reduce and limit the impact on individuals and early notification of a breach is key to protecting the interests of the individual.

Furthermore, obligations placed upon USWCS/the University under the General Data Protection Regulations require that **breaches of personal data must be reported to the Information Commissioner's Office within 72 hours and failure to do this could result in USWCS being subject to fines of €10,000,000**. It is therefore imperative that all breaches are reported promptly in accordance with this procedure.

For further information on data protection and definitions relating to key terms please refer to the data protection pages on www.uswcommercial.co.uk/about/privacy-statement.

## Purpose

This procedure informs those who handle personal data on behalf of USWCS of the steps they must take in the event of an incident where personal data/a system holding personal data has been lost or compromised.

This procedure ensures that a consistent approach is in place for dealing with and responding to a data breach and information security incidents within USWCS.

## Scope

This procedure applies to all Individuals (as defined in USWCS Data Protection Policy) handling USWCS information and information assets.

## Personal data

Personal data is defined as information relating to an identified or identifiable person and may include (but is not limited to):

- Factual information about an individual such as date of birth, national insurance number, bank account, name and address.
- Sensitive information such as health, sexual life, criminal record, ethnicity, religion.
- Opinions expressed, for example in staff development reviews or email comments.

**Definition of an incident**

A personal data security breach is defined as:

> "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

This includes both information in hard copy and electronic information. Breaches include (but are not limited to):

- Where there is a loss of access to personal data held e.g. it has been prematurely destroyed, damaged or corrupted and no further copies are held.
- Theft or loss of data e.g. sensitive papers or a laptop containing personal data being lost.
- Instances where personal data is altered either in error or without authority.
- Accidental disclosure/unauthorised disclosure e.g. personal data being emailed to the wrong person (whether internal or external to USWCS) or published online/where an Individual uses USWCS controlled personal data for an unauthorised purpose.
- Malicious access to data e.g. student personal data being given out to an impostor over the telephone or hacking.
- Unauthorised access to a USWCS/University system/account e.g. an Individual making available their password to a third party as a result of deception/phishing.

**Action to be taken**

Where a breach has been identified the Individual who has identified the breach must immediately submit a notification through the University to the Information Compliance Manager Breaches must be reported to IT Services immediately and no later than 12 hours after the Individual becomes aware of the incident.

<u>If an Individual suspects that a breach has occurred, it is expected that a cautious approach is taken and that a report is submitted to POB.</u>

The following information must be provided:

- An explanation of the nature of the breach and factors leading up to the breach.
- Confirmation that the breach is contained.
- What is the nature of the data (personal/sensitive personal and detail of type of information)?
- Whose data has been breached?

- What is the quantity/volume/number of users affected?
- Have any complaints been received.
- What measures have been put in place to mitigate?
- How much/many data/people have been affected by the breach?
- Who are the people whose data has been breached?
- Likely consequences of the data breach.
- A means to contact the Individual to discuss the matter.
- The name of the Individual's Line Manager or Engager.

**USWCS actions**

Once a breach notification has been received by the University's Information Compliance Manager, (the "Information Compliance Manager") will consider how to respond in line with the IT Security Incident Management Procedure.

**Non compliance with this procedure**

Failure to report a data breach is a breach of USWCS Data Protection Policy and Individuals will be subject to action.

**Links to other policies and procedures**

This document should be read in conjunction with:

USWCS Data Protection Policy
Relevant University Polices

# Email and personal data guidance

USW Commercial Services Ltd ("USWCS") has a responsibility under data protection laws to ensure that personal data is kept secure from unauthorised disclosure, that is personal information or data is only disclosed to those who are authorised to receive it.

The General Data Protection Regulations provides new powers to the Information Commissioner who can impose fines of up to €20,000,000 (or up to 4% of turnover – whichever is greater) on organisations who do not comply.

The guidance has been prepared to assist all Individuals responsible for personal data in ensuring that the risks of unauthorised disclosure of such data are minimised.

- Never redirect or forward emails from your University account to your personal account such as a g-mail or Hotmail account. Data may be stored outside of the EU and consequently Individuals may, if personal data is involved, be in breach of the data protection laws.

- When sending emails Individual must ensure, prior to pressing the 'send' button that it is being sent to the correct recipient.

- Individuals must check that they are sending the correct attachment and that the only information being sent is the information that is necessary. Individuals must check carefully that the attachment contains only the information that needs to be distributed e.g. on spreadsheets Individuals must check for 'hidden' columns and additional tabs that may contain information that should not be distributed.

- Highly sensitive or confidential data must not be sent in the body of the email. Such data must only be included in an encrypted attachment.

- Where personal data is sent via an encrypted document, the password must not be sent within the e-mail or by a separate e-mail – Passwords must be exchanges face-to-face or by telephone only to the individual to whom the e-mail has been sent.

- Individuals must not share their passwords to access their IT accounts with anyone.

- Where Individuals send emails containing personal information to the wrong recipient all incidents must be reported to the Data Protection Officer using the data breach procedure.