DATA PROTECTION AND DATA DISPOSAL POLICY

Department	Strategic Planning		
Author	Legal Advisor		
Authorised By:	Associate Director for Strategic Planning		
Implementation By:	Data Protection Officer		
Policy Reference:	POSP1718010		
Policy Replaced:	POAR1617006		
Version No:	1	**Approval Committee:**	VCB
Date approved:	09.07.18	**Minute no:**	17.139.02
Status:	Approved	**Implementation Date:**	July 2018
Period of approval:	3 years	**Review Date:**	July 2021

I have carried out an equality impact assessment screening to help safeguard against discrimination and promote equality.	
I have considered the impact of the Policy/Strategy/Procedure *(delete as appropriate)* on the Welsh language and Welsh language provision within the University.	

1. Introduction

This policy forms part of a suite of policies and procedures that support the University information governance framework.

The University needs to hold and to process large amounts of personal data about its students, employees, alumni, contractors, suppliers and other individuals in order to carry out its business functions (this list is not exhaustive).

Data Protection law defines 'personal data' as 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 particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental economic, cultural or social identity of that natural person.

2. Purpose

Compliance with legislation will be achieved through the implementation of controls and responsibilities including measures to ensure that:

2.1 personal data is processed lawfully, fairly and transparently. This includes the provision of appropriate information to individuals upon collection of their data by the University in the form of privacy notices. The University must also have a legal basis to process personal data. The legal basis for processing is outlined within Article 6 of the General Data Protection Regulations.

2.2 Personal data is processed only for the purposes for which it was collected

2.3 Personal data is adequate, relevant and not excessive for the purposes for which it was collected

2.4 personal data is accurate and where necessary kept up to date

2.5 Personal data is not kept for longer than necessary

2.6 Personal data is processed in accordance with integrity and confidentiality principles, this includes physical and organisational measures to ensure that personal data, both manual and digital, are subject to an appropriate level of security when stored, used and communicated by the University, in order to protect against unlawful or malicious processing and accidental loss, destruction or damage, It also includes measures to ensure that personal data transferred to or otherwise shared with third parties have appropriate contractual provisions applied;

2.7 Personal data is processed in accordance with the rights of individuals, where applicable. These eight rights are:

- **The right to be informed**
  The University must provide individuals with information about the data processing activities we carry out. This information is provided within the Student, Staff and Generic Privacy Notices. The information must be, concise, transparent, intelligible and easily accessible; written in clear and plain language and free of charge.

  www.glyndwr.ac.uk/cy/informationGovernance/Policies/.
  www.glyndwr.ac.uk/en/informationGovernance/Policies/

- **The right of access to the information held about them by the University (through subject access request)**

  The University must provide individuals with confirmation that their data is being processed and how to access their personal data. The University must comply with any subject access request within one month of receipt at no charge unless the request is manifestly unfounded or excessive.

- **The right to rectification**

  The individual can have their personal data rectified if it is inaccurate or incomplete. The University must comply with any request to rectify within one month. This can be extended to two months where the request is complex

- **The right to erase**

  Individuals have the right for their data to be erased where the personal data is no longer necessary for the purpose for which it was collected or processed. The University must comply where the individual withdraws their consent or objects to the processing and there is no overriding legitimate interest to continue processing or the personal data was unlawfully processed or has to be erased in order to comply with a legal obligation. However, the University can refuse to erase where it is processed due to an exemption, to exercise a right of freedom of expression and information, comply with a legal obligation or for the performance of a task of public interest or for the exercise or defence of legal claims and for purposes relating to public health, archiving in the public interest, scientific/historic research or statistics. This also includes if there has been disclosure to a 3rd party.

- **The right to restrict processing**

  Individuals have the right to restrict processing of personal data where they have contested its accuracy, they have objected to the processing and the University is considering whether the individual has a legitimate ground which overrides this, the processing is unlawful and the University no longer needs the data but the individual requires it to establish, exercise or defend a legal claim. This also includes informing 3rd parties to erase the personal data

- **The right to data portability**

  Individuals have the right to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits. It only applies to personal data the individual has provided to the University; where the processing is based on consent or the performance of a contract and where processing is carried on by automated means. The personal data must be in a structured, commonly used and machine readable form (e.g. CSV files) and if the Individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. The University must comply with the individual request free of charge and within one month. This can be extended to two months where the request is complex or if there are a number of requests

- **The right to object**

  Individuals have the right to object to processing based on legitimate interest, the performance of a task in the public interest or the exercise of official authority (including profiling). Also, direct marketing (including profiling) and processing for scientific/historic research or statistics. The University must inform the individual of their right to object as soon as possible and where the individual does object to direct marketing they must do so immediately as there are no exemptions or grounds to refuse, Where the individual objects to the processing of their data, the University must comply with this request unless the University can demonstrate overriding compelling legitimate grounds to continue processing or that the processing is for the establishment, exercise of defence of legal claims

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

  Individuals have the right not to be subject to a decision when it is base d on automated processing; and it produces a legal effect or a similarly significant effect on the individual, The University must ensure that data subjects are able to obtain human intervention, express their point of view and obtain and explanation of the decision and challenge it. Profiling is any form of automated processing intended to evaluate certain person aspects of an Individual, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour and location. This would not apply if the automated decision is necessary for entering into or performance of a contract, is authorised in law (purposes of fraud or tax evasion) is based on explicit consent or does not have a legal or similarly significant effect on the individual. The University must ensure that appropriate safeguards are in place if processing personal data for profiling purposes and must be fair and transparent about the logic involved, use appropriate mathematical/statistical procedures, implement appropriate technical and organisational l measures to correct inaccuracies and minimise the risk of errors.

2.8 The design and implementation of University systems and processes must make provision for the security and privacy of personal data

2.9 Personal data will not be transferred outside of the European Economic Area (EEA) without the appropriate safeguards in place

2.10 Additional conditions and safeguards must be applied to ensure that more sensitive personal data (defined as special category data in the legislation), is handled appropriately by the University. Special Category personal data is personal data relating to an individual's:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union memberships
- Genetic data
- Biometric data (where used for identification purposes)
- Health; or
- Sex life or sexual orientation

In addition, similar extra conditions and safeguards also apply to the processing of the personal data relating to criminal convictions and offences. The University classification scale can be found at

www.glyndwr.ac.uk/cy/informationGovernance/Policies/
www.glyndwr.ac.uk/en/informationGovernance/Policies/

3. Scope

This Policy applies to:

- All personal data held and processed by the University. This includes expressions of opinion about the individual and of the intentions of the University in respect of that individual. It includes data held in any system or format, whether electronic or manual.

- All members of staff, as well as individuals conducting work at or for the University and/or its subsidiaries, who have access to University information ("staff"). This includes temporary, honorary, visiting, casual, voluntary, fellows, Board members and agency workers, students employed by the University and suppliers and sub-contractors (this list is not intended to be exhaustive); and
- All locations from which personal data is accessed including off-campus

4. Responsibilities and compliance framework

All staff and other approved users of the University systems must:

- Complete data protection training every two years, and must seek advice and guidance from the Data Protection Officer if clarification is required; and

- Immediately report to your Manager, Associate Director, Director, Dean of Faculty, the SIRO, who is the senior information risk officer, accountable for assurance of information security at the University (SIRO@glyndwr.ac.uk) and the Data Protection Officer dpo@glyndwr.ac.uk of any actual or suspected misuse, unauthorised disclosure or exposure of personal data, 'near misses' or working practices which jeopardise the security of personal data held by the University.

The University has a serious information governance incident procedure ('SIGI') outlining the process the University undertakes when a breach of data has been reported. This procedure can be found at www.glyndwr.ac.uk/en/informationGovernance/Policies/

Deans of Faculties, Associate Directors and Directors (known as Information Asset Owners) are responsible for ensuring that personal data within their area is processed in line with this Policy and established procedures. To assist with this the University has identified Information Asset Administrators across the Faculties and professional functions. The Faculty Business Managers will further support their Faculty on information governance.

The Information Asset Administrators ("IAA") will be responsible for overseeing data protection compliance in their areas where applicable. The IAA will identify local training needs and arrange for them to be met via the Data Protection Officer. The IAAs are also responsible for helping to identify circumstances where data sharing or transfer agreements are needed with third parties and ensuring that these are put in place, copies of which need to be sent to the Data Protection Officer for placing on a register.

The Data Protection Officer is responsible for providing procedures, guidance and advice in support of this policy and for training staff. The Data Protection Officer is further responsible for overseeing the University compliance with the data protection legislation.

If any employee, officer or student of Glyndŵr University creates their own system or record, for example a spreadsheet or database/card index, whether computerised or on paper which contains personal data, this must be consistent with the permitted uses identified above and managed with the appropriate level of security. Any ambiguity regarding intended uses of personal data should be notified to the Data Protection Officer www.dpo@glyndwr.ac.uk who will ensure it complies with the above requirements and appropriate security is applied to it.

Provided that the identification of individuals cannot be ascertained or is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data.

Staff must note that any breach of this Policy may be treated as misconduct under the University's relevant disciplinary procedures and if proven, could lead to disciplinary action or sanctions. Serious breaches of this Policy may constitute gross misconduct and if proven, lead to summary dismissal or termination of contract.

5. Glyndŵr University must adhere to its personal data retention policy

Glyndŵr University must not keep information for longer than is necessary for the purpose for which it is being processed, which includes as long as may be necessary for the purpose of defending any legal proceedings brought against the University in relation to the processing or as required by law, any regulatory body or recommended by any relevant code of practice. Further information regarding retention of personal data can be obtained from the Data Protection Officer and can be found within the Records Management Policy www.glyndwr.ac.uk/cy/informationGovernance/Policies/
www.glyndwr.ac.uk/en/informationGovernance/Policies/

The Data Protection Officer will review the nature of information being collected or held periodically to ensure there is a sound business reason requiring the information to be held.

6. Monitoring compliance

This policy and its implementation are subject to internal monitoring and auditing throughout the University, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. The Information Governance Committee ("IGC") will receive quarterly reports and have oversight of the University Information Governance policies and procedures and will undertake any appropriate benchmarking.

7. Review of Policy

This Policy will be reviewed by the Information Governance Committee as and when required or when legislation dictates.

8. Contacts

Data Protection Officer is Leonna Messiter and can be reached by email on dpo@glyndwr.ac.uk

9. Complaints

If an individual is dissatisfied with the way, the University has handled her/his personal information or has requested personal information held about her/him (Subject access request) and has not received a reply, a complaint may be made.

This complaint should be submitted in the first instance to the Associate Director of Strategic Planning and should provide a brief explanation of the reasons for the dissatisfaction. The complaint will be acknowledged immediately and the Associate Director of Strategic Planning will provide a fuller response within 15 working days.

If the complainant remains dissatisfied following this response, she/he may seek an independent review from the Information Commissioner.

The University's notification number is **Z5199192.**

DATA DISPOSAL

1. SCOPE OF POLICY

It is Glyndŵr University's policy to:

- dispose of data using methods which meet fully the requirements of the Data Protection Act.
- display a general duty of care to the disposal of data such that no individual or organisation is compromised by material which has not been correctly destroyed.
- use cost-effective and environmentally-friendly disposal mechanisms, appropriate to the media involved.

2. INTRODUCTION

This policy deals with the disposal of personal data stored in Glyndŵr University records. It is necessary to have such a policy to ensure that methods of data disposal meet the requirements of the Data Protection Act. Glyndŵr University's personal records are usually based on paper, computer (CD, data tape, memory stick etc.), or videotape (for CCTV), but may take other forms. It is important that the correct method of disposal is used both in regard to the medium on which the record is stored and the type of personal information that is being destroyed.

Glyndŵr University's compliance with the Data Protection Act is a key reason for the establishment of a data disposal policy for personal information. However, it must be realised that **any** University data that is not correctly disposed of, and is later on uncovered and made public, could cause embarrassment, controversy and adverse publicity for Glyndŵr University. This data disposal policy is therefore necessary regardless of the legal requirements placed upon us.

Additional care must be taken when disposing of sensitive personal data.

Terminology: note that "disposal" is used in preference to "deletion" since it is associated with all types of media, whereas "deletion" is more usually applied to electronic and paper records only.

3. APPLICATION

The policy is to be used where there is a risk that personal data that is no longer required could become accessible to a third-party if it is not disposed with appropriate care. The policy is not intended to apply when ad-hoc deletions are made in local files where there are no security implications: for example, when small groups of records are being erased in a personal spreadsheet.

Please note that the policy does not deal with preferred retention periods of records, nor with archiving policies, nor does it deal with differences in record types (medical, financial, disciplinary etc.): it is only concerned with methods used for disposing of data. The retention schedule which deals with how long information should be held for can be found in The Records Management Policy

www.glyndwr.ac.uk/cy/informationGovernance/Policies/
www.glyndwr.ac.uk/en/informationGovernance/Policies/

4. DELEGATING RESPONSIBILITY

4.1.1 Third parties

You must not delegate responsibility for disposal of personal information to a third party except in the following cases:

- you have a clear agreement with an internal department that they will take full responsibility for disposal of specific records (e.g. where for technical reasons IT Services have agreed to delete records from computer disks using specialist tools or where Campus Services operate a confidential waste disposal service).

- you are making use of a formal written agreement with an external party for the disposal of data (e.g. using confidential shredding services).

- There may be occasions when there are 3rd parties processing data on our behalf. Upon termination of the contract or agreement with the 3rd party, the University needs to ensure that those 3rd party suppliers dispose of the personal data they hold on our behalf appropriately and securely. There should be reference to how the 3rd party will dispose of the personal data within the contract or agreement the University has signed. It is imperative that this is checked by you upon termination.

Data management

When an agreement or contract has been terminated, you need to be assured that data held on 3rd party systems have been disposed of securely. It is recommended that you should contact the 3rd party and seek formal clarification that disposal has been carried out and how this has been completed. This clarification should be inserted into the information asset register for data management purposes.

4.2 Desktop Computers, Laptops and other Devices with Electronic Storage

Never assume that someone else will delete information on your behalf if you are passing on a Device with Electronic Storage internally within Glyndŵr University. You should make your own arrangements for the removal of all personal records from computers for which you have no further use: you should not rely on a subsequent user to take that responsibility unless this has been clearly agreed.

Please be advised that removable media USB sticks will need to be encrypted via appropriate software security systems dependent on the devices being used, for example ‘bitlocker’ for Microsoft Office systems. It is your responsibility to ensure that all removable media storage has been encrypted appropriately.

5. STEPS FOR DATA DISPOSAL

a) Check that the proposed disposal of personal data is in line with your department’s data retention guidelines: this will differ greatly depending on the type of personal information involved (for further information please refer to the Records Management Policy and associated Record Retention schedule or contact the Data Protection Officer).
b) Ensure that there are no relevant proceedings in progress relating to individuals identified in the data: for instance, internal disciplinary action, contract disputes or court actions.

c) Identify and use the appropriate means of disposal below:

Records stored on a Desktop, Laptop or similar electronic device (where the device is to be re-used)

If the relevant records form only a part of a database, spreadsheet or similar file, then removal of those records using the internal erasure procedure of the relevant program is acceptable. For example, you can use the 'Row deletion' function in Excel to delete the relevant records and you need take no further action.

If you require complete removal of data files which do not contain sensitive personal data the standard Windows or other operating system tools are adequate, but this assumes that the device will continue to be in the use of the current user for the foreseeable future, otherwise the file wiping approach must be used, as follows.

File wiping is required in particular where files containing sensitive personal information (see above) are to be removed. In this case you cannot safely use the file deletion tools in Windows Explorer or Apple IOS to remove Windows files (e.g. Excel, Access and Word files). This is because it is generally straightforward with a little technical knowledge to retrieve files that have been deleted in this way. Instead, a file-wiping utility should be used: this can be undertaken by IT Services who you should contact to provide assistance.

Records stored on a Desktop, Laptop or similar electronic device (where the device is not expected to be re-used)

Where the device storage is not to be used in the future, physical destruction of the device must be performed (regardless of the type of personal information they contain). IT Services ensure this is performed for all equipment which is to be disposed of.

Network based computer records

The standard file deletion routines are sufficient for network-based files. If there is extreme sensitivity regarding the information which is being deleted you should liaise with IT Services to ensure that backup tapes containing archive copies of these files are appropriately handled.

Paper and microfilm

The minimum standard for the destruction of paper and microfilm containing personal information should be shredding using shredding machines provided by the university. The task of shredding should only be delegated where confidentiality of the operation can be assured. Alternatively, the records may be placed in the care of a confidential waste disposal operator, with whom Glyndŵr University has entered a written agreement to dispose of the material to the necessary standard.

Please note that paper records of this nature should never be placed in a waste-bin or a non-confidential waste recycling bin without prior shredding.

Tapes (including data tapes and videotapes)

Where they are to be reused tapes may be overwritten with non-personal images or blank information, or subjected to degaussing. If they are not to be reused tapes must be physically

destroyed to the point that the carrier cartridge is not serviceable and the tape cannot practically be re-used.

Memory Sticks, Tablet, Mobile Phone memory and similar

Methods of disposal of records will vary by device type for memory sticks, tablets etc. You should contact IT Services for advice where permanent erasure is necessary. Where the disposal process is part of a record 'weeding' policy and sets of records are being deleted according to the University's Records Retention schedule then the activity should be recorded in a departmental register of disposals (please refer to the Data Protection Officer for further information). This is intended to demonstrate to the Information Commissioner's Office (i.e. the agency responsible for implementing Data Protection legislation) that proper safeguards have been observed. Note that it is not necessary to record deletions unless they are part of a routine purging operation. The following information should be recorded:

General particulars, *ie type of information, such as tuition fee records for 2013*

- Date of disposal
- Means of disposal, e.g. shredding
- Responsible officer