FFURFLEN MANYLION POLISI
POLICY IDENTIFICATION FORM /FRONTSHEET

TEITL Y POLISI: *POLICY TITLE:*	**DATA PROTECTION (GDPR)**
UWCH-GYFARWYDDWR A CHYFRIFOLDEB: *RESPONSIBLE EXECUTIVE DIRECTOR:*	*Corporate Services*
PWRPAS: *PURPOSE:*	*This is Grŵp Llandrillo Menai's statement of intent towards the responsible compliance with the General Data Protection Regulation (GDPR) and related EU and national legislation, and Data Protection Act 2018*
OBLYGIADAU RISG: *RISK IMPLICATIONS:*	*Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, access to Grŵp Llandrillo Menai facilities being withdrawn, financial penalties for the Grŵp, and criminal prosecution.*
EFFAITH AR DDWYIEITHRWYDD *IMPACT ON BILINGUALISM*	*No impact*
EFFAITH AR GYNALIADWYEDD *IMPACT ON SUSTAINABILITY*	*None*
ARGYMHELLIAD: *RECOMMENDATION:*	*For review*
CYFATHREBU *COMMUNICATION*	*Via Timau Polisi, Strategol, and Rheoli to all staff.*
PWLLGOR / GRŴP MONITRO: *COMMITTEE / GROUP RESPONSIBLE FOR MONITORING:*	*Audit & Risk Committee* *Finance and Resources* *Board*
CYMERADWYWYD GAN: *APPROVED BY:*	*Corporation Board*
DYDDIAD CYMERADWYO *APPROVAL DATE:*	**27.06.19**
DYDDIAD ADOLYGU *REVIEW DATE CYCLE:*	*Annual*

GENERAL DATA PROTECTION REGULATIONS – STATEMENT OF INTENT FOR GRŴP LLANDRILLO MENAI

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

As a Data Controller, the Grŵp needs to collect and process information including personal information about the people that it deals with in order to operate effectively and efficiently. These include current, past and prospective students, employees, partners, suppliers, clients/customers, and others with whom it communicates with in order to monitor student enrolment, retention and attainment, maintain staff records and provide performance reporting.

In addition, it may be a legal requirement to collect and use certain types of information, for example to comply with the requirements of government departments for student, staff or business data. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are strengthened safeguards to ensure this in the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act2018.

The Grŵp regards the lawful and correct treatment of personal information as essential to successful operations, and to maintaining confidence with those it deals with. The Grŵp will ensure that it treats personal information lawfully and correctly.

All personal data, however collected must be processed in accordance with the Eight Principles of the GDPR; this applies equally to data recorded in automated systems, manual files and other storage media such as pen drives, micro fiche and CCTV.

To ensure the lawful processing of personal information, anyone processing personal data must comply with the eight enforceable principles of good practice, which state that personal data shall:

1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the data subject's rights.
7. Be kept safe from unauthorised access accidental loss or destruction.
8. Not be transferred to a country outside the European Union, unless that country has equivalent levels of protection for personal data.

1. Definitions

Grŵp Purposes	The purposes for which personal data may be used by us: Students, personnel, administrative, financial, regulatory, payroll and business development purposes. *College business purposes include (but are not limited to) the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice in carrying out our duties as an education provider.* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring Corporate and user policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of official sensitive information, security vetting, and checking.* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and reviews* - *Monitoring staff conduct, disciplinary matters* - *Communication with the public*
Personal data	Information relating to identifiable individuals, such as students, clients, customers, job applicants, current and former employees, current and former Governors, agency, contract and other staff, clients, suppliers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV. (This list is not exhaustive and further information is available in the Grwp's Privacy Statements viewable here.*

Special categories	Special categories data includes an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. *Any use of special categories data must be strictly controlled in accordance with this policy. Special categories also includes biometrics, DNA, facial and fingerprint recognition.*
Data Controller and Data Processor	The data controller is the person or entity (in this case the Grŵp) that determines the purposes for which, and the way in which, personal data is processed.

	By contrast, a data processor is anyone who processes personal data on behalf of the data controller (excluding the data controller's own employees)

2 Scope

This policy applies to all staff, contractors, and agency workers employed by the Grŵp. **You must be familiar with this policy and comply with its terms.**

This policy supplements our other information governance policies, which are all located on the intranet. These policies include:

- IT usage policy
- Internet acceptable use policy
- Email acceptable use policy
- Data Protection Privacy Notices and Guidance

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be approved through Tîm Strategol and the Corporation Board, and then circulated to staff.

3 Who is responsible for this policy?

The protection of data is everybody's responsibility. Accountability for compliance with Data Protection within the Grŵp is ultimately the responsibility of the Executive Director for Corporate Services. The Data Protection Officer (DPO) has overall responsibility for the day-to-day implementation and review of this policy.

3.1 The Executive Director for Corporate Services Data Protection responsibilities:

- Establish an effective Information Governance Framework for the Grŵp
- Act as the executive level champion for information within the Grŵp
- Ensure information assets and risks within the authority are managed
- Promote compliance with statutory, regulatory and organisational information policies
- Establish a reporting and learning culture to allow the organisation to establish where problems exist and to develop strategies to prevent future problems occurring.

3.2 The Data Protection Officer's responsibilities (DPO):

- to inform and advise employees about the Grŵp's obligations to comply with the Data Protection Act 2018 / GDPR and other data protection laws;
- to monitor compliance with the Data Protection Act 2018 / GDPR and other data protection laws, and with data protection policies, including managing internal data

protection activities; raising awareness of data protection issues, training staff and conducting internal audits;

- to advise on, and to monitor data protection impact assessments;
- to cooperate with the supervisory authority (ICO); and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

3.3 Data Protection Support Officer:

- Assisting the DPO in the day-to-day functions of ensuring compliance with Data Protection
- Acting at the key service link between the DPO and staff
- Regular review and upkeep of the service information asset register
- Processing and co-ordination data protection policies
- Processing data subject requests.

3.4 Responsibilities of the Director of IT:

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the authority is considering using to store or process data

4 Principles

The data protection legislation and principles set out the main responsibilities for organisations.

Personal data shall be:

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

2) 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;
3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) 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;

5) 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 Data Protection Act 2018 in order to safeguard the rights and freedoms of individuals; and

6) 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.

The ability to **demonstrate compliance** is a key change which everyone processing personal data must comply.

5. Procedures

5.1 Privacy Notices - transparency of data protection

Data protection legislation states that we must have privacy notices that are *specific* to activity which requires personal information.

The privacy notice:

- Sets out the purposes for which we hold personal data
- Highlights that our work may require us to give information to third parties
- Provides that citizens have a right of access to the personal data that we hold about them

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following questions must be answered when processing personal data:

What information is being collected?
Who is collecting it?
How is it collected?
Why is it being collected?
How will it be used?
Who will it be shared with?
List the identity and contact details of any data controllers
List the details of transfers outside of EEA (European Economic Area) and safeguards

5.2 Personal Data

We must process personal data fairly and lawfully in accordance with individuals' rights.

The lawful basis for processing personal data requires that at least one of the following conditions **must** apply whenever you process personal data:

a. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
b. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
d. **Vital interests:** the processing is necessary to protect someone's life.
e. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply to public authorities processing data to perform official tasks.)

5.3 Special Categories data

Special category data is personal data which is more sensitive, and so needs more protection. In order to lawfully process special category data, you must identify both a lawful basis for processing personal data (see para 6.2) and a separate condition for processing special category data as outlined below. These two conditions do not have to be linked.

There are currently ten conditions for processing special category data but additional conditions and safeguards may be added. You must determine your condition for processing special category data before you begin this processing, and you must document it.

In most cases where we process special categories data we will require the data subject's consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The lawful basis for processing special categories data requires that in addition to the conditions listed in paragraph 6.2, you must also apply at least one of the following conditions whenever you process special categories data:

a) **Explicit consent of the data subject,** unless reliance on consent is prohibited by EU or Member State law.

b) Necessary for the **carrying out of obligations** under employment, social security or social protection law, or a collective agreement.
c) Necessary **to protect the vital interests** of a data subject who is physically or legally incapable of giving consent – this is the equivalent of the wording in the DPA.
d) Processing carried out in the course of its **legitimate activities with appropriate safeguards** by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
e) **Data manifestly made public** by the data subject.
f) Necessary for the **establishment, exercise or defence of legal claims** or where courts are acting in their judicial capacity.
g) Necessary for reasons of **substantial public interest** on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures – this means that Member States can extend the circumstances where sensitive data can be processed in the public interest.
h) Necessary for the purposes of **preventative or occupational medicine,** for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
i) Necessary for **reasons of public interest in the area of public health,** such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
j) Necessary for **archiving purposes in the public interest, or scientific and historical research** purposes or statistical purposes.

6 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask us to correct inaccurate personal data relating to them.

We will make it clear to citizens that they must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required. This will be communicated through the Grŵp's Privacy notices.

7 Data security

Staff, agency staff, contractors and Governors must protect personal data and keep it secure, to prevent loss or misuse. Where other organisations process personal data as a service on our behalf, services must liaise with the DPO to establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

8 Storing data securely

a. In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
b. Printed data should be shredded when it is no longer needed and/or disposed of using confidential waste sacks
c. Data stored on a computer must be protected by strong passwords.
d. Data stored on external devices must be encrypted and locked away securely when they are not being used
e. Any cloud used to store data must have the prior approval of the Director of ICT.
f. Servers containing personal and special categories data must be kept in a secure location.
g. Data held on the Grŵp's systems will be regularly backed up
h. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
i. All personal and special categories data stored on the company's IT systems must be identified and handled in line with the ICT Usage Policy.

9 Data Retention

We must retain personal and special categories data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our **Retention Schedule Guidance** at the end of this document.

10 Information Sharing

The Data Protection Act is not a barrier to sharing information but rather provides a framework to ensure that personal information about living persons is shared appropriately. Staff should not hesitate to share personal information in order to prevent abuse or serious harm, in an emergency or in life-or-death situations. If there are concerns relating to child or adult protection issues, then the relevant procedures should be followed.

The Wales Accord on the Sharing of Personal Information (WASPI) was developed in 2011 as a practical approach to multi agency sharing for the public sector in Wales.

Information sharing is key to joined up service delivery. Decisions on whether to share information must be taken on a case-by-case basis, which should then be supported by the production of either an Information Sharing Protocol (ISP) or a Data Disclosure Agreement (DDA). Each new ISP and/or DDA must have a clearly defined purpose for the sharing and must

be seen and registered by the Data Protection Officer before being signed off at Directorate Level.

11 Transferring data internationally

There are restrictions on international transfers of personal and special categories data. You must not transfer personal and special categories data anywhere outside the UK without first consulting the Data Protection Officer.

12 Data Subject's Rights

Data Protection legislation provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

12.1 The right to be informed

Individuals have the right to know that information about them is being processed. This is done through a privacy notice. The information that must be supplied is determined by whether or not the Grŵp obtained the personal data directly from individuals. The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and free of charge.

12.2 The right of access (subject access requests)

Individuals are entitled, subject to certain exemptions, to request access to information held about them. If you receive a subject access request, you should refer that request immediately to the Data Protection Officer.

We will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the designated departmental data protection lead about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the Data Protection Officer for advice on direct marketing before starting any new direct marketing activity.

12.3 The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the personal data in question has already been to third parties, we must inform those third parties of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

We must respond within one month. This can be extended by two months where the request for rectification is complex. Where we are not taking action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the Information Commissioner's Office, Information Commissioner's Office Wales, 2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH.

12.4 The right to erasure (also known as the right to be forgotten)

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies. We must respond within one calendar month.

12.5 The right to restrict processing

We will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether the authority's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- We may need to review procedures to ensure we are able to determine where you may be required to restrict the processing of personal data.

If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. We must also inform individuals when we decide to lift a restriction on processing.

12.6 The right to data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free. The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

12.7 The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

12. 8 Rights in relation to automated decision making and profiling.

Data Protection legislation makes provisions for:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The legislation applies to all automated individual decision-making and profiling. There are additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or law applicable to the controller; or
- based on the individual's explicit consent.

You must identify whether any of your automated decision making has legal or similarly significant effects on them. If so, make sure that you:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

13 Protection of children and vulnerable people

Where information is passed to the Grŵp concerning safeguarding, then the risk posed and the individual's right to privacy will have to be balanced against each other.

If information received by the Grŵp relating to any person(s) who may come into contact in any way with children and/or vulnerable persons raises concerns as to the appropriateness of the person(s) having contact with children and/or vulnerable people and/or as to the future well-being of such children and/or vulnerable persons, the Grŵp will consider it a duty to share that information. It may be shared with any appropriate individual, company group, committee, Police Force, Local Authority or agency if the balance of risk is deemed to require the sharing of such information.

Grŵp Llandrillo Menai deems the duty to safeguarding vulnerable people as an over-riding duty to the duty to protect information.

14 Imagery

The Grŵp will ensure, where necessary, that all the people who will appear in a photograph, video or web cam image are made aware that such recording is taking place, with the exception of CCTV. The Grŵp will also make clear why it is using that person's image, what it will be used for.

Legal guidance states that by the age of 13 a child may be considered to have `sufficient maturity' to understand their rights under the Act.

However, The Grŵp has decided that parental/guardian consent should be sought up to the age of 18 years.

15 Training

All staff and Governors will receive e-learning training on data protectionNew starters will receive this training as part of the induction process. Further training will be provided at least every three years or whenever there is a substantial change in the law or our policy and procedure. Training will be accessed through the Grŵp Staff Development Programme and/or Network Applications.

It will cover:

- The law relating to data protection
- Data protection and related policies and procedures.

Completion of training is mandatory for all staff.

16 Privacy by design and default

Privacy by design is an approach to projects, processes or activities that promote privacy and data protection compliance from the start. The Directorate initiating a new project, process or activity will be responsible for conducting a Privacy Impact screening and if necessary a full assessment.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

17 International data transfers

No data may be transferred outside of the EEA without first discussing it with the DPO.

18 Information Asset Register and data audit

Each Directorate will nominate a **data protection lead** who is responsible for the regular review and up keep of the service information asset register. Regular data audits to manage and mitigate risks will inform the data register. The asset register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

19 Reporting breaches

All members of staff and Governors have an obligation to report actual or potential data protection non-compliance **as soon as possible** to the DPO. This is necessary to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- If necessary, notify the Information Commissioner's Office (ICO) within 72 hours of any compliance failures that are material either in their own right or as part of a pattern of failures.

20 Consequences of failing to comply

Grŵp Llandrillo Menai takes compliance with this policy very seriously. Failure to comply puts both individuals and the institution at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our employment procedures, which may result in dismissal. A failure in compliance may also lead to a fine being imposed upon the Grŵp.

Staff Checklist for Recording Data

- ✓ Do you really need to record the information?
- ✓ Is the information 'standard' or is it 'sensitive'?
- ✓ If it is sensitive, do you have the data subject's express consent?
- ✓ Has the data subject been told that this type of data will be processed?
- ✓ Are you authorised to collect/store/process the data?
- ✓ Are you sure that the data is secure?
- ✓ If yes, have you checked with the data subject that the data is accurate?
- ✓ If not, do you have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- ✓ Have you reported the fact of data collection to the authorised person – DPO?

Further reading/references to be found on Grŵp Portal – Policies, Procedures & Documents Tile:

"Data Classification Protocol 2016" - ICT
"Encrypting Pen Drives or Hard Drives Using Bitlocker" – ICT
"ICT Access Entitlement and Remove Protocol" – ICT
"ICT Usage Protocol Staff" – ICT
"Information Security Protocol" – ICT
"Mobile Device & Teleworking Protocol" – ICT"Grŵp Safeguarding Policy" – Quality & Students

APPENDIX 1 TO THE DATA PROTECTION POLICY

Staff Guidelines regarding disclosure of information about Learner/ Staff to third parties.

Introduction

Any information relating to a living person and which can be identified as referring to him/her is covered by the Data Protection Act 2018/GDPR, whatever the format – electronic, paper, file tape, text etc.

Personal Data is categorised as:

Standard Personal data – name, address details about class attendance and coursework, marks and grades, plus notes of personal tutorials.

Sensitive Personal data has to be handled with special care and includes details of:

- Details of ethnic or racial origin; political opinions; religious beliefs; trade union membership or non-membership; physical or mental health; sexual life; criminal record.
- Records containing payroll, pension, of any individual.
- Higher level personal data including staff/student disciplinary details.
- Records containing information relating to an individual's home or family life, personal finances or a personal reference.

Collecting Information

The Grŵp has consent from the individual for retaining staff and student information in the Standard Personal data category.

The only piece of Learner Sensitive Personal data that is covered by the standard learner disclaimer on the enrolment form is the issue of ethnic or racial origin. All other data on for example family life or personal finance can not be retained without the data subject/individual's agreement.

Staff are forbidden to share any Personal Information with third parties.

The same applies to Staff Sensitive Personal data. In order to monitor equal opportunities or social economic trends ethnic or racial origin, information is retained as is payroll, pension and next of kin details. Any other such details – disciplinary, personal finance etc. – could not be retained (outside Standard policy) without express individual permission.

Medical Information

Programme areas may need to be informed when Staff or Learners are unable to attend Grŵp Llandrillo Menai on health grounds, or otherwise affected by ill-health. Great care needs to

be taken when dealing with medical information. This type of information should only be dealt with on a 'need to know' basis, and this may, for example, result in such matters being dealt with by a sub-section of a group rather than the full membership of a committee or other meeting. Any correspondence or documentation relating to health issues should only be posted under confidential cover, and details of illness should not as a rule be discussed over the telephone or via e-mail. Medical notes should not be left on desks, or circulated except under confidential cover. Care must be taken when transmitting this, or any other sensitive material by fax or electronic media.

Examination/Assessment Results

Care should be taken that strict confidentiality and secure office practices are followed while papers are being marked and while results are being compiled. The Data Protection Act 2018 /GDPRdoes not give students the right to access their own examination scripts (but the Act does say that they can access comments made upon them by examiners). However, they will be able (under subject access rights) to see the breakdown of marks awarded for particular questions, or sections of examinations. Permissible sanctions in cases of student debts or return of library books include withholding awards, certificates or permission to re-register; however, their marks or results cannot be withheld. It has been confirmed that the display or pass/fail lists on noticeboards is indeed permissible under the Act. However, individual students must be removed from these lists if they so request.

Noticeboards and Websites

In order that Grŵp Llandrillo Menai is able to carry out its legitimate business, it is permissible to publish lists of staff with their photographs, responsibilities and contact details within Grŵp Llandrillo Menai. It is also permissible to display staff photographs on Staff and Student Identification Badges as a means of ensuring the health, safety, security and safeguarding of all Grŵp staff and students.

References

The regulations give an individual the right to ask Grŵp Llandrillo Menai for a copy of a reference received about them (subject to whether the reference may reveal information about a third party), but not those provided by Grŵp Llandrillo Menai. However, there is nothing to prevent an individual requesting access to a reference provided on behalf of Grŵp Llandrillo Menai from the body or person to whom it was provided. Confidential references received by Grŵp Llandrillo Menai are not exempt from the provisions of subject access request. However, consideration should be given to the rights of the referee and consent should be sought.

Staff need to take care when preparing references, which should be factually accurate and must not give a misleading impression overall. This may mean putting certain facts into context so that the references as a whole is true, accurate and fair. Matters of opinion should be based on factually accurate data. References should be written on the presumption that the employee will gain access to a copy of the document. The same principles should apply for internal references, correspondences and reports.

Release of Information

Internal Enquiries

Standard Personal Data can be passed between authorised personnel in Programme Areas and Corporate areas in order for them to carry out the business of Grŵp Llandrillo Menai. Utmost care must be taken with sensitive personal information, such as medical details, promotion cases etc., where information should only be provided on a 'need to know' basis.

Any personal data sent using the internal mail system should be sealed and sent under 'Confidential' cover. Examples include probation reports, enrolment forms.

In most cases, it is likely that the enquirer will be known to you and you will not be in any doubt about his/her identity. However, there will be cases where you are contacted by an enquirer where you only have the say-so of that person that they are a member of Grŵp Llandrillo Menai staff. Where you receive such an enquiry by telephone, it is recommended practice to call the enquirer back on a verifiable phone telephone number. For in-person enquirers, you should ask to see the staff ID card as proof of entitlement. For written enquiries, check that the enquirer is an employee and entitled to the information by reviewing Grŵp portal information.

External Enquiries

'External' enquiries are defined as anyone who does not meet the criteria above. **Such enquiries must be treated with great caution**. The Grŵp receives regular requests for information on students both past and current. The main thing to remember is that according to the Data Protection Act 2018 /GDPR, the circumstance under which personal information can be disclosed without the authorisation of the individual are fairly limited.

For example, addresses (including e-mail addresses) or telephone numbers must NOT be released to any third parties, even if they claim to be close friends or family members. In emergencies, staff can contact the student or member of staff themselves, and pass on messages.

In general:

- If the request comes from the police, immigration service, Inland Revenue or similar official body, the enquirer should be referred to Data Protection Officer.
- Any requests from the press or media should always be referred, **without comment**, to the Chief Executive Officer or Principal
- Information on studentsor groups of students must not be released to other students.
- All requests from trade unions, which includes enquiries by individual trade unionists that are staff members, should be referred to the Human Resources Director.
- Bodies or organisations requesting personal information on students must make a written request and such requests should be discussed with the relevant manager and referred to the DPO.

Parents/Spouses/Other Relatives

Information can be passed to parents or guardians if the student is under 18 at the **start of their programme of learning.** If a student is 18 or over at the start of their programme of learning, information should not be passed to their parents or guardians. The request should then be discussed with the student. If the student agrees that information can be passed to their parent/guardian then they should sign an information release form as confirmation. Once the form has been signed, you may comply with any future requests.

The Grŵp has no obligation to provide information to other family members. Grŵp procedures, however, may be discussed freely with anyone. Thus it is possible to explain to a parent, in principle, the process for retaking an examination etc. but not to divulge the specific circumstances of an individual's case without the agreement of the student.

Sponsors

Sponsors and similar bodies (private companies, charities etc.) do not have a right to access 'their' students' Personal Data (even if they are paying the tuition fees). Students must have signed a data release form before you can release the information. However, details on attendance patterns and progress may be passed to the sponsor as stated on the student enrolment forms.

The Data Subject

Although students and staff have a general entitlement to access the records Grŵp Llandrillo Menai holds about them, they have no right to demand to see your records *immediately,* without having first made a proper application, through the Grŵp's DPO

Exceptional Circumstances

Confidentiality may have to be breached if there is danger that:

- The data subject may harm him/herself.
- The data subject may harm other persons.
- The data subject's life or health and safety may be threatened.

Professional Accreditation

It has been the practice in some Programme Areas to provide lists of final results to professional bodies to assist them in awarding professional accreditation to eligible candidates. We have been advised by the Office of the Information Commissioner that this practice is illegal unless each individual listed has given express consent that their details may be passed on. Express consent is defined as a positive response to an enquiry and cannot be inferred by failure to object by a deadline.

Statutory Bodies

Grŵp Llandrillo Menai is obliged to release information on all its students and staff to the Welsh Government (WG). These returns are made by Registry and Human Resources on behalf of Grŵp Llandrillo Menai. Information is provided on each individual member of staff or student, but is collected and processed by WG so that educational statistics can be compiled and national trends monitored. The information collected and held by WG, is of course, subject to the confidentiality conditions of the Data Protection Act.

Information is also provided to such bodies as examining bodies, the Student Loans Company, Careers Wales, Franchised Universities and Local Education Authorities (this list is not exhaustive). These reports are dealt with by the appropriate central administrative offices, and Programme Areas are asked to refer any requests for information from any statutory bodies to the Data Controller as appropriate. A data release form must be signed by the relevant manager before the release of information to statutory bodies or other organisations.

There are other bodies which Grŵp Llandrillo Menai is obliged to pass information to by law but all information collected is subject to the confidentiality conditions of the Data Protection Act.

Past Students and Staff Records

As we are obliged to discard material if it no longer meets a legitimate need, information held on past students and staff needs to be edited so that only relevant details are retained. Grŵp Llandrillo Menai is often approached by people wishing to contact their former colleagues. In these circumstances the usual confidentiality rules apply: personal details may not be passed on to any third party, but Grŵp Llandrillo Menai may agree to pass messages on to the students or staff concerned. The Registry Manager is the central point of contact for all such student requests, and the Human Resources Director for all staff requests.

Staff Responsibilities

All staff should be aware of and follow the above guidelines, and seek further guidance where necessary. These Guidelines should be read in conjunction with the Grŵp Llandrillo Menai Data Protection Policy, and staff should note that breaches of the Policy may result in disciplinary action.

Data Protection Queries

Grŵp Llandrillo Menai has a Designated Data Protection Officer who acts as Grŵp Llandrillo Menai liaison with the Office of the Information Commissioner and is the point of contact to whom any queries regarding data protection matters should be addressed. This person is Toby Prosser, Director of Governance and Information.

Any requests from Data Subjects to access their own records under the terms of the Data Protection Act should also be addressed to the DPO. Subject Access Requests must be made using the appropriate pro-forma (available from the DPO). The group will aim to respond to

each request within one month of receipt of the application. In the unlikely event that this is not achieved a full explanation will be given.

APPENDIX 2 - RECORDS MANAGEMENT POLICY 2019:

1. Requirements for a Records Management Policy:

Grŵp Llandrillo Menai recognises that efficient management of its records is essential both for effective administration and to enable it to comply with legal and regulatory requirements. Records held by the Grŵp have always had legal significance, as for example, proof of the terms of a contract or evidence for employment law purposes. In recent years, however, records themselves have become the focus of legislation, notably in the Data Protection Act 2018 , General Data Protection Regulations (GDPR), Freedom of Information Act 2000 (FOIA).

These guidelines establish requirements to help staff meet their legal obligations relating to records management and to manage records so that their value as a corporate resource for the Grŵp is fully exploited.

2. Standards for management of records within the Grŵp:

- Each Department will implement procedures for record management and keep them under critical review in order to ensure that best practice is followed and records are stored cost effectively.
- Records must be appropriately accessible and retrievable.
- Records maintained will be accurate, timely and version controlled.
- Security of records must be consistent with their confidentiality and importance.
- Retention and disposal of records will be governed by the retention schedule agreed by the Grŵp available at Annex C.

Documents of significance to the history of the Grŵp will be retained indefinitely e.g. Minutes of Corporation Board, Articles of Association, Audited Annual Accounts and relevant published materials.

3. Scope of the guidance:

Records are defined as any information resource providing evidence of transactions and activities of the Grŵp. They can be in hard copy or electronic form.

All records created and received by staff in the course of Grŵp business are owned by Grŵp Llandrillo Menai as a corporate body and not by the individual departments, sections or teams that create or hold the records.

The Grŵp owns the intellectual property and copyright of all records created by staff.

Records must not be removed from Grŵp premises/systems or used for any activity other than the purpose for which they were provided and retained. Records must not be deleted or destroyed except in accordance with this Records Management Policy.

4. Implementation of Ownership

- Senior staff, Assistant Principals, Directors and Programme Managers will be responsible to the Chief Executive Officer for the implementation of this policy within Grŵp Llandrillo Menai.

- The Data Protection Officer is responsible for drawing up guidance for good records management practice and promoting compliance with the policy.

- All members of staff are responsible for ensuring that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the standards laid down.

Annex B gives advice on good records management practice.

5. Guidance

Advice on the procedures necessary to comply with this policy will be available from the Data Protection Officer. This guidance will cover:

- Records creation and receipt
- Filing schemes
- Retention periods for records
- Security and storage options
- Disposal of records
- Access to stored records
- Relevant legislation and external codes of practice.

6. Objectives of a Record Management System

Records contain information that is a valuable resource and important operational asset. A systematic approach to the management of the College records is essential to protect and preserve records as evidence of actions.

Records management is necessary to:

- Ensure that the College conducts itself in an orderly, efficient and accountable manner
- Deliver services to staff and stakeholders in a consistent and equitable manner
- Support and document policy formation and managerial decision making
- Provide continuity in the event of a disaster
- Meet legislative and regulatory requirements

- Provide protection and support in litigation including the management of risks associated with the existence or lack of evidence of organisational activity
- Protect the interests of the organisation and the rights of employees, clients and present and future stakeholders
- Establish a business and cultural identity and maintain a corporate memory.
- Maintain/store in the most economical way consistent with the above objectives.

Useful Contacts:

Data Protection Officer:
Toby Prosser
(Director of Governance and Information)
data@gllm.ac.uk
01492 546666 Ext 1313

Data Protection Support Officer:
Caroline Jones
(Grŵp Clerking Officer)
01492 546666 Ext 8658

Head of Registry:
Sam Walsh
s,walsh@gllm.ac.uk
01492 546666 x 1217

Assistant Director of Finance
Alison Evans,
a.evans@gllm.ac.uk
01492 546666 x 1221

Head of ICT:
Aidan Sheil
a.sheil@gllm.ac.uk
01492 546666 x 1285

Freedom of Information Officer
Toby Prosser
(Director of Governance and Information)
t.prosser@gllm.ac.uk
01492 546666 Ext 1313

Records Management

Annex A

What is Records Management?

The National Archives guidance on records management defines a record as "information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or transaction of business". One important thing to note about records management is that it aims to cover records of all formats and media. It should also be stressed that records management needs to be carried out throughout the record's existence. The process does not begin when a record is transferred to an archive store, it begins with the decision to create the record.

Benefits of good records management:

Records are one of Grŵp Llandrillo Menai's most valuable assets. They are vital for routine, day-to-day tasks and they support decision-making. They also document the aims, policies and activities of the College and ensure that legal, administrative and audit requirements are met. Records build up a collective memory and support the image of the College which is presented to the outside world.

In order to perform these functions, records must be managed well. There must be control over what is created and effective and efficient filing systems to store the records in. It must also be ensured that records that are still needed are kept in cost-effective, secure storage and that those no longer needed are destroyed appropriately. This in turn will save money on storage, reduce misfiles, lead to quicker retrieval of records and make day-to-day work simpler and easier.

Annex B

Advice on good records management

- ✓ Why you need to keep the data?
- ✓ Have an organised approach to record-keeping
- ✓ Share information strictly in accordance with Data Protection Act 2018 / GDPR principles, password protected
- ✓ Ensure that you are able to locate and retrieve records when required
- ✓ Be able to provide evidence of activities, decisions and actions
- ✓ Ensure adherence to relevant legislation
- ✓ Keep what you need only for as long as is required (depending on administrative, legal or statutory requirements).
- ✓ Ensure long-term preservation of records of archival value to maintain the corporate memory.

REMEMBER:

GOOD RECORDS MANAGEMENT IN THE GRŴP DEPENDS ON THE EFFORTS OF ALL STAFF

Annex C

Retention Policy

From the various Acts the following retention periods will be established for College records.

However, please note EU funded projects will always override minimum retention periods. See 5.11 below and Annex D.

5.1	Health & Safety: The Health and Safety at Work Act 1974 stipulates:		
A.	Risk Assessment	Review of risk	+ 3 years
B.	Monitoring of working environments	Date of creation of document	+ 40 years
C.	Control and use of hazardous substances	Document Closure	+ 40 years
D.	Monitoring of employees' health	Creation of document	+ 40 years
E.	Accident Books	Date of closure of book	+ 3 years
F.	Accident/dangerous occurrence report forms	Date of occurrence	+ 3 years
G.	Categorising and disposal of waste	Creation of document	+ 3 years
	The Limitation Act 1980 stipulates:		
A.	Reporting and investigation of accidents and dangerous occurrences	Date of accident	+ 40 years
B.	Conduct of testing, maintenance and statutory inspections and any necessary action	Life of equipment/plant	+ 6 years
C.	Maintenance schedules	Date of creation of document	+ 2 years
D.	Inspection certificates	Date of creation of document	+ 6 years
E.	Repair reports	Life of equipment/plant	+ 6 years
5.2	Estates: The Health & Safety at Work Act 1974 stipulates:		
A.	Categorising and disposal of waste	Creation of document	+ 3 years
	The Limitation Act 1980 stipulates:		
A.	Conduct of testing, maintenance and statutory inspections and any necessary action	Live of equipment/plant	+ 6 years
B.	Maintenance Schedules	Date of creation of document	+ 2 years
C.	Inspection Certificates	Date of creation of document	+ 6 years
D.	Repair reports	Life of equipment/plant	+ 6 years

However, please note EU funded projects will always override minimum retention periods. See 5.11 below and Annex D.			
5.3	Personnel: The Health & Safety at Work Act 1974 stipulates:		
A.	Monitoring of employees health	Date of creation of document	+ 40 years
	The Sex Discrimination Act 1975 and 1986, the Race Relations Act 1976 and the Disability Discrimination Act 1995 stipulate:		
A.	Advertising of vacancies	Filing of vacancy	+6 months
B.	Successful job applications	Transfer to staff personnel file	
C.	Unsuccessful job applications	Filing of vacancies	+6 months
D.	Ethnic monitoring questionnaires and reports (Race Relations Act 1976)	Date of creation of document	+ 5 years
	The Limitation Act 1980 stipulates:		
A.	Disciplinary hearings against staff	Date of settlement of case	+ 6 months (unless the document is merged with the staff personnel file
B.	Staff personnel files	Date of termination of employment	+ 6 years
5.4	Finance: The Limitation Act 1980 stipulates:		
A.	Procurement records – successful tenders	End of supply contract	+ 6 years
B.	Procurement records – unsuccessful tenders	Date of creation of document	+ 1 year
C.	Lettings of student accommodation	End of agreement	+ 6 years
D.	Hiring out of conference facilities	End of agreement	+ 6 years
E.	Private hire agreements	End of agreement	+ 6 years
F.	Insurance policies	End of policy	+ 6 years
G.	Insurance claim	Settlement of claim	+ 6 years
H.	Payroll payments	Date of creation of document	+ 6 years
I.	Share certificates (if appropriate)	Date of disposal of shares	+ 6 years
J.	Investment portfolio reports (if appropriate)		Indefinitely
	The Companies Acts 1985 and 1989 stipulate:		
A.	Accounts	Date of creation of document	+ 6 years
B.	Records of dissolved companies	Date of dissolution	+ 10 years
	The Financial Services Act 1986 stipulates:		

However, please note EU funded projects will always override minimum retention periods. See 5.11 below and Annex D.			
A.	Salary details	Current financial year	+ 6 years
	The Value Added Tax Act 1994 stipulates:		
A.	Purchase Orders/ invoices	Date of creations of document	+ 6 years
B.	Delivery notes/goods received notes	Date of creations of document	+ 6 years
C.	Income and expenditure accounts	Date of creations of document	+ 6 years
D.	Management of bank accounts/ statements	Date of creations of document	+ 6 years
E.	Assessment of tax liabilities	Current tax year	+ 6 years
F.	Submission of tax return	Current tax year	+ 6 years
5.5	Purchase Officers: The Limitation Act 1980 stipulates:		
A.	Procurement records – successful tenders	End of supply contract	+ 6 years
B.	Procurement records – unsuccessful tenders	Date of creation of document	+ 1 year
	The Value Added Tax Act 1994 stipulates:		
A.	Purchase orders/ invoices	Date of creation of document	+ 6 years
B.	Delivery notes/goods received notes	Date of creation of document	+ 6 years.
5.6	Payroll: The Limitation Act 1980 stipulates:		
A.	Payroll payments	Date of creation of document	+ 6 years
	The Financial Services Act 1986 stipulates:		
A.	Salary advices	Current financial year	+ 6 years
5.7	Conference Activity: The Limitation Act 1980 stipulates:		
A.	Hiring out of conference facilities	End of agreement	+ 6 years
5.8	Corporate Services: With reference to intellectual property (if appropriate) The Limitation Act 1980 stipulates:		
A.	Control of disclosure of intellectual property	Date of disclosure	+ 6 years

However, please note EU funded projects will always override minimum retention periods. See 5.11 below and Annex D.			
B.	Administration of intellectual property agreements	End of agreement	+ 6 years
C.	Intellectual property agreements	End of agreement	+ 6 years
D.	Claims of infringement of intellectual property	Date of settlement of claim	+ 6 years
5.9	MIS: The management, retention and disposal of student records, including records of examinations and qualifications are as listed in 5.10		
5.10	Curriculum Areas: The management, retention and disposal of student records, including records of examinations and qualifications are listed below under the following awarding bodies		
	Type of Record	Retention Period	
	Coursework & Portfolios of evidence	No requirement to retain once student has received certification.	
	Other candidate evidence	Kept by the candidate in their portfolio	
	* Exam records	Receipt	+ 3 years
	* Student assessment records (at unit level)	Completion	+ 3 years
	* Assessor records	Completion	+ 3 years
	* Internal Verifiers records	Completion	+ 3 years
	* External Verification records	Completion	+ 3 years
	* Work placement documentation	Completion	+ 3 years
	Certificates	If not collected immediately	+ 1 year and return to awarding body
	* "These records need not be actual raw data of what candidates achieved but summary records to identify what was assessed, when it was assessed, what assessment decision was reached, who assessed, who internally verified".		
5.11	**Busnes@**		
	All EU funded project documents under the Convergence Programme 2007-2013 and the EU programme 2014-2020 are to be retained until confirmed by WEFO – earliest date available is 2024 but confirmation by WEFO takes precedence. See Annex D		

ANNEX D

Document retention policy for European Structural Funds projects

1. This policy relates to the retention of documentation in relation to project activity that is funded through the European Structural Funds 2014-2020 (ESF, ERDF, RDP or other funds). It will be updated periodically to reflect any changes in European Regulations, which currently state that: "For a period of three years….following the payment by the Commission of the final balance in respect of any assistance, the responsible authorities shall keep available for the Commission all the supporting documents (either the originals or versions certified to be in conformity with the originals on commonly accepted data carriers) regarding expenditure and checks on the assistance concerned."

2. In line with European regulations, the length of time required to retain documents is not a definitive date. However, guidelines published by the Welsh European Funding Office suggest a destruction date of no earlier than 2025.

3. All documentation should be retained relating to European funded projects in-line with the above statements and for the purposes of audit as required. No documents should be destroyed without the following:

    - A notification from the Welsh European Funding Office (WEFO) that the final payment has been received from the European Commission
    - An official letter from the Welsh European Funding Office (WEFO) or project lead sponsor approving the destruction of project documentation

4. For the purpose of this policy, project documentation includes paper originals and those stored electronically, and includes but is not limited to, the following;

    - Financial records
    - Beneficiary records
    - Policy documents
    - Projects procedures
    - Evaluations
    - Staff records
    - Procurement/tendering records
    - Project documents
    - Project activity [INSERT ORGANISATION LOGO]
    - Publicity
    - Cross-cutting themes.

Annex E

How to Store Records

If you are planning to store records in an Archive you only need to follow these 3 easy steps:

1. Complete a Records Transfer List
2. Box up the records
3. Arrange for collection by caretakers (and ensure space is available in your archive area).

Transfer lists and flat-pack boxes and lids are supplied on request from the Estates Department.

Records Transfer Lists

The Records Transfer List is a vital document. It is your guide to what has been transferred in each box and the Service's guide to what is in the Archive Store. Accuracy is important.

When the boxes arrive at the Archive Store they should be allocated a location reference. This will be added to the transfer list, and a copy returned to the office as well as one held in the Archive Store location. This is the reference number you should use when seeking the return of a file.

Completing the list – hints

The lists should be completed in triplicate. The format should be Box Number, File Title/Covering Dates, Retention Period, Date for Destruction (if appropriate).

Box Number Use this column for your own box number which will also be marked on the boxes. for example if you're depositing 10 boxes they could be marked 1-10.

File Title Most titles are self-explanatory e.g. "Schools relations", "Admission policies", "Student dossiers". Some are self-explanatory now, but won't be in a couple of year's time, e.g. "Mandy and Caroline: Meetings", or "CSSA". If you have a filing system based on codes (egB4/11), will using the reference alone be enough to identify the file in future? For student files, you don't need to list individual names where files are already in alphabetical or numerical order. Use "Student files A-E".

Covering dates These are the dates of the earliest and most recent items on the file.

Retention period This is the period for the length of time the documents should be retained. For guidance on this see the Retention Schedule at Annex C.

Boxing records – hints:

Instructions for making up the flat pack boxes and lids are available from the Estates Department.

Don't fill the box to bursting point. If you can't lift the box then it is too heavy for archiving. There is no charge for storage so you won't be saving your department any money by overfilling the boxes.

You will probably find it easier to box and list at the same time. As you go, try to reduce the bulk of the file. For example:

- ✓ Have you weeded the file? You can destroy duplicates, drafts, printed reports.
- ✓ Have you cleared the sleeves of duplicates, drafts, printed reports?
- ✓ Loose papers often proved to be duplicates, old (unfilled) filing, or just plain rubbish. Don't forget the recycling bin.
- ✓ Please take out any plastic wallets or covers, as these will be difficult to destroy when the file reaches the end of its lifespan.

If the filing system has been neglected, you can often destroy files yourself there and then. For example copy Board and Committee minutes are held centrally and then archived. Records such as old order copies and outdated suppliers' information are of no use to anyone.

Mark the side of the boxes with the references you've given them on the Transfer List. i.e. Box 1, Box 2 etc.

Confidential destruction:

The Estates Department will collect material to be confidentially destroyed. This shredding is carried out off-site by a commercial company. They shred and bale the paper before it is delivered to a paper mill for final pulping. Bags for confidential waste can be obtained from the Estates Department.

All plastic wallets or covers of any kind must be removed as this material melts in the shredding machine and the company we use will refuse to take the bags.

Confidential waste sacks should only be used for confidential materials.

NOTE: We only collect confidential waste, i.e. material containing personal or commercially sensitive information. If you have other documents that need to be destroyed these can be recycled using the paper recycling boxes (from Estates department) (Again no plastic items to be included).

Equality Impact Assessment

Date: May 2018

Policy / Procedure/Process Title: DATA PROTECTION POLICY

Personnel Involved in Equality Impact Assessment:

Consideration	Response	Further evidence requirements	Outcome
Which protected groups might be disadvantaged by the policy/process	The Data Protection Act 2018 / GDPR requires the college to ensure that it takes particular steps to protect the confidentiality of sensitive personal data as defined by the Act. The Grŵp is compliant with this requirement. The way in which information is then provided in response to subject access requests made under the Data Protection Act 2018 / GDPR is set out by the legislation. It has not been possible to identify any adverse impact arising specifically from the procedure.	**Monitoring of to ensure that no specific groups of staff or learners are disadvantaged**	
Which protected groups might benefit from the policy/process	**All groups protected under the GDPR 2016 and Data Protection Act 2018**		
Does the policy advance equality and foster good relations	**Yes – the policy will encourage the legal and fair processing of data.**		
Could any part of the process discriminate unlawfully	**Not if the policy is fully adhered to.**		
Are there any other policies that need to change to support the effectiveness of this one	**No – other relevant policies in place**		
Conclusion: Tick one	~~**Adjust the Policy**~~	**Continue the Policy and process**	~~**Stop and Remove the Policy**~~
Please list:			
Date Actions to adjust completed	**[]**		

Signed: Bryn Hughes Parry

Date: May 2018

Welsh Language Impact Assessment Name of Policy or Procedure: GDPR POLICY Date: May 2018
Personnel/Groups Involved:

Consideration	Response	Further evidence requirements	Outcome
What **positive effects** will the implementation of the policy or procedure have on the use of Welsh language?	The policy will ensure that each member of staff will be aware of their responsibilities to be compliant with the GDPR 2016 and Data Protection Act 2018and will be published in both Welsh and English. Individuals should be aware that their data will be held in Welsh and/or English and if they wish to discuss their data that they can do so in Welsh or English.		
What **negative effects** will the implementation of the policy or procedure have on the use of Welsh language?	None		
Are there **sufficient Welsh-speaking staff** available to implement the policy or procedure? If not, what steps will be taken to ensure that sufficient staff are available, and by when?	Yes – in accordance with the Grŵp's Welsh Language Plan. The procedure should be adhered to by all Grŵp staff. Where an individual makes a request to speak about personal data or issues relating to the Data Protection Act 2018 / GDPR, there are sufficient staff in Governance, Registry and in HR to be able to provide that service in Welsh.		
Does the policy or procedure comply with **Grŵp Llandrillo Menai's Welsh Language Schemes/Language Strategy?**	Yes		

Conclusion	~~**Adjust the policy or procedure**~~	**Continue the policy or procedure**	~~**Stop and remove the policy or procedure**~~

Signed: Bryn Hughes Parry Date: May 2018