Coleg Gŵyr Abertawe
Gower College Swansea

DATA PROTECTION POLICY

Issue	**December 2020**
Review Date	**November 2022**
Originator	**Sharon Barron** **Data Protection Officer**
Location of Policy	**BIZ-Sharepoint / Intranet / Policies & Procedures / Information Security and MIIS**
Policy Approved by:	**Information, Governance & Security Group – 10 November 2020** **JNCC- 20 November 2020** **Audit Committee – 3 December 2020** **CMT – 17 December 2020**

1. Overview

Gower College Swansea is committed to meeting its obligations under the General Data Protection Regulation (GDPR) which came in to force in May 2018. This policy sets out Gower College Swansea's approach to the way it stores, handles and allows access to information about its employees and students.

2. Background

The College is required by law to comply with the General Data Protection Regulation. It is also registered with the Information Commissioner's Office where it notifies them of the purposes for which it intends to process personal data.

The GDPR applies to personal data which is defined as information relating to an identified or identifiable natural person. It gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly by those responsible for obtaining, holding or otherwise processing it. Processing is defined very broadly and includes the collection, retention, use and disclosure of information

The General Data Protection Regulation states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legal purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that it is inaccurate and is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it was processed;
- 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 College is responsible for, and must be able to demonstrate, compliance with the above principles.

In addition, GDPR also provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Individuals, who feel they are being denied proper access to their personal information or feel this information is not being handled according to the principles of the General Data Protection Regulation, can contact the Information Commissioner's Office for help. Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.

Failure to comply with the General Data Protection Regulation will, in some instances, constitute a criminal offence. Non-compliance will be investigated by the Information Commissioner's Officer and fines may be applied for the non-compliance.

3. Context

Gower College Swansea needs to collect, process, keep and use certain types of information about people with whom it deals in order to carry out its day to day functions. These people include current, past and prospective students, customers, staff, partners, Corporation members, suppliers of goods and others. This personal information, whether on paper, on a computer, or recorded on other material, must be used fairly and processed in accordance with the GDPR. The data must also not be disclosed to any other person unlawfully.

All staff and students should be aware:-

- that all **personal data** collected, held, and processed (including Internet software) whether in manual, digital, electronic or any other format is **subject to the GDPR**

- of the circumstances under which they may or may not legitimately **access, process and disclose personal data**

Note – Individuals, including staff and students, in relation to whom the College holds information are referred to as **"data subjects"**

The College is a body corporate and the Board of Governors is therefore ultimately responsible for compliance with the General Data Protection Regulation. The day to day operation of this policy is undertaken by the Data Protection Officer. The Data Protection Officer for Gower College Swansea is **Sharon Barron.**

The Data Protection Officer reports to The Board of the Governors and is independent of the management and data owners of the College.

Any issues in interpretation or application of this policy should be directed, in the first instance, to the Data Protection Officer.

If a Subject Access Request (SAR see below) requires access to network systems (e.g. personal E-mail, personal drives) then Computer Services will release the information only upon authorisation from the Data Protection Officer and relevant data owners to ensure that management of the data request conforms to the principles of the GDPR. Access to the information will then be under the supervision of the Computer Services Manager.

4. Scope

This policy applies to all staff, students, partner organisations, subcontractors, suppliers and visitors and all other parties granted access to College data and information. It includes all information/data relating to living individuals that is collected, processed and stored by the College.

This policy applies to requests by individuals for information about themselves as well as to specific requests for personal information relating to others.

The principles set out in this policy are also relevant to other related policies and procedures e.g. CCTV, Absence Monitoring, Data Protection Impact Assessment Procedure, Data Breach Notification, Information Security Policies, etc.

All staff must complete mandatory regular training on their responsibilities within GDPR. Guidance on the policy, for staff and students, is available via the Intranet and at enrolment (students) and induction (staff).

All third parties must be made aware of our policies and agree to comply with them.

Responsibilities of Staff

It is a condition of employment that employees should comply with policies and procedures of the College. Failure to observe this Data Protection Policy may therefore lead to disciplinary action; serious or deliberate breach of the rules may be regarded as gross misconduct. Breach of this policy may in some circumstances constitute a criminal offence.

All staff need to be familiar with:

- what personal information they can and cannot collect
- what personal information they can and cannot store
- how and for how long the information should be stored
- what information can and cannot be disclosed
- to whom information can be disclosed and in what format
- the College's data classification scheme

If there is any doubt as to whether the data should be collected, processed or stored, this should be discussed with the College Data Protection Officer.

All staff have a responsibility in relation to the accuracy of information relating to themselves that is held by the College. Staff are required to

- ensure that any information that they provide to the College in connection with their employment is accurate and up to date.
- inform the College of any changes to information, which they have provided, such as changes of address.
- inform the College of any errors in information held about them by the College. The College cannot be held responsible for such errors if it has not been made aware of them by the staff member concerned.

Any member of staff who believes that the policy has not been followed in respect of their personal data should firstly raise the matter with the relevant data owner. If this cannot be resolved the matter should be referred to the College's designated Data Protection Officer.

All staff using the College's computer facilities must realise that the GDPR applies whenever personal data is being processed. Examples of processing can occur through email, social media and learning platforms e.g. Office 365. The data protection principles still apply when processing hard copy personal data in letters, assessments and other documents.

5. Responsibilities of Students

The College requires all students to provide informed consent to the processing of their personal data for educational, administrative and welfare purposes and to comply with this Data Protection Policy.

Students must ensure that all personal data provided to the College is accurate and up to date. Change of details forms are available via reception or, in some instances, changes can be notified electronically.

Students using the College's computer facilities must realise that the General Data Protection Regulation may apply wherever the personal data of other individuals is being processed. This is particularly likely to arise where information about other individuals is being made available to others on line. For example, when corresponding via e-mail, using social media, and when using or creating web pages. The data protection principles still apply when processing hard copy personal data such as correspondence and other documents.

6. General Principles for Collecting & Processing Data

The College (including its employees and students) is required to process personal data only where there is a legitimate purpose for doing so, and then only as necessitated by that purpose.

The College is required by law to notify the Information Commissioner of the purposes for which it intends to process personal data. This annual notification is published on the Data Protection Public Register. It is the responsibility of the Data Protection Officer to update this notification annually in the light of any changes to the retention, use and disclosure of information.

The College will provide a Privacy Notice at the point information is collected and processed which will inform data subjects of the purpose of collecting the information, the lawful basis for collection, with whom it will be shared, how long it will be kept and the data subject's rights

Sensitive and Highly Sensitive Personal Data

Sensitive and Highly Sensitive personal data are special categories of personal data and includes data about:-

- the racial or ethnic origin of the data subject
- political opinions
- religious or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sex life
- sexual orientation
- genetic and biometric data (where processed to uniquely identify individuals)

The College operates a data classification system that has four categories:

	Public	Internal	Sensitive	Highly Sensitive
Restricted		x	x	x
Non-restricted	X			

Guidance relating to the above classification system is included within the Information Security Data Classification Guidelines (available on the College intranet).

Data relating to the commission or alleged commission of any offence or proceedings for any offence or alleged offence are not categorised as sensitive personal data but must be processed with the same level of safeguards as sensitive personal data.

Agreement to the processing of certain personal data (e.g. previous criminal convictions) is a condition of acceptance of a student onto any course, and a condition of employment for staff in line with the Child Protection and Vulnerable Adult Policy and the Unspent Criminal Convictions Policy.

Prospective staff and students will be asked to sign a consent form, regarding the use of information when an offer of employment or a course place is made. This will include express consent for the types of sensitive information the College has to collect and process. Refusal to sign such a form could result in the offer being withdrawn in line with the Policies above.

Data Protection Impact Assessments

When introducing new systems or procedures the College will consider whether personal data is affected and if so carry out a Data Protection Impact Assessment (DPIA). Where as a result of a DPIA it is clear that the College is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not to proceed must be escalated to the DPO. The DPO shall, if there are significant concerns, either as to potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

Obtaining Consent

The College obtains informed consent to process and release data at the point at which it is being collected. For example through the student application / enrolment form and the staff job application form / contract of employment. Students are also given a “Privacy Notice” which explains rights and responsibilities and third parties with whom data is shared and the purpose for releasing this data.

7. Data Breaches

A personal data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Where it is identified that a data breach may have occurred (whether by accident, loss or through malicious intent) then the breach must be reported to the relevant data owner and the Data Protection Officer. (Data Breach Notification Process)

The Welsh Government requires notification within 24 hours of discovering a breach involving any work based learning related data.

Action should be taken to mitigate the breach wherever possible. Should this require authorisation to access the College email system authorisation must be provided by the Principal/Deputy Principal or a member of the CMT if neither of these are available.

The Data Protection Officer will report the breach to the Information Commissioner's Office (if applicable) within 72 hours and ensure that individuals affected by the breach are informed (if applicable).

8. General Principles for Information Security

All staff (and students, where applicable) are responsible for ensuring that:

- Any personal data that they hold on behalf of the College is kept securely.
  - Paper records should be stored in a locked drawer or filing cabinet.
  - Information stored on a computer should be password protected
  - Digital & magnetic media used for storage or backup purposes should, be password protected and, where appropriate, encrypted
  - Particular care must be taken in respect of the physical security of portable media (e.g. disks and data sticks) or laptop computers carrying personal data. Such devices must hold data in an encrypted form and be approved by the Computer Services department

- Personal information is not disclosed in either verbal or written form, deliberately or accidentally to any unauthorised third party.

- Under no circumstances must information be released about an individual to any person requesting this information by phone, fax or post unless the identity of the person making the request and their entitlement to receive the information requested has been confirmed. **Parents (other than in the case of children under 16 and vulnerable adults who lack capacity to make relevant decisions), spouses, partners, children and employers of students are <u>not</u> entitled to information about another individual – without express consent from the individual concerned**

- Any third party who process that information on behalf of the College must comply with the GDPR, agree to a data sharing protocol or sign up to a Wales Accord on the Sharing of Personal Information (WASPI).

- Personal data must only be accessed internally by those with a legitimate purpose for doing so and should not be disclosed to external agencies without proper authority from the individuals concerned or with the approval of the College's Data Protection Officer.

- Casual disclosure does not take place by for example leaving computer printouts uncovered on desktops or by allowing unauthorised users to view computer screens. Computer printouts must be kept securely and destroyed in a confidential manner.

- College offices where the processing of personal data takes place should be locked when not occupied.

- Staff should not take equipment, information or software off-site without prior authorisation.

- Staff (and students where applicable) should take particular care with personal data while working remotely – considering particularly:-
  - Nature of the data – is it personal? Am I allowed to take it home?
  - Who might be able to see the data – family members; fellow travellers on public transport?
  - Security of the data – both in electronic and paper format
  - Physical security of portable media
  - Use of password and encryption measures as appropriate

Further detailed information is provided in the Information Security Policy and its associated policies and procedures.

All staff and students are responsible for ensuring that they observe the IT policies and procedures of the College

Staff and students are required to notify the College immediately where they become aware that personal data in their possession has been lost, stolen or damaged so that the College can carry out appropriate risk assessment and take any necessary corrective action in accordance with current Information Commissioner guidance.

Sensitive material should be placed in confidential waste bins/ bags, where ever possible shredded, and disposed of as confidential waste by the Estates Department. This would include anything relating to learner records, exam matters or staffing matters. Particular care should be taken to delete information from computer hard drives if a machine is to be disposed of or passed on to another member of staff\department**.**

9. General Principles of Disclosure

Disclosures will be permitted only where data subjects have **given their informed consent**, or where the GDPR permits transfers without such consent.

The College must ensure that personal data under its control is not disclosed to unauthorised third parties. These include:

- A person or organisation to whom the data subject has not consented that the data be disclosed, unless the 2018 Data Protection Act expressly permits such transfers without such consent (see below)

- A person or organisation to whom the data subject has consented that the data be disclosed, but where the request is for reasons other than that for which the data was collected, or for which the consent was given, unless the 2018 Act expressly permits such transfers without such consent (see below)

"Unauthorised third parties" will include family members, friends, local authorities, government bodies, and the police, unless disclosure without consent is permitted by the 2018 Act (see below), or by other legislation. **There is no general legal requirement to disclose information to the police.** For further guidance, staff should refer to the College's Data Protection Officer.

Disclosure without Consent

Data may be disclosed to third parties **without consent**, in some circumstances, for example for the:

- purpose of protecting the vital interests of the data subject and the data subject is not able to give consent (i.e. release of medical data where failure to release the data would result in harm to, or the death of, the data subject)
- purpose of preventing serious harm to a third party that would occur if the data were not disclosed
- purpose of safeguarding national security
- prevention or detection of crime including the apprehension or prosecution of offenders
- apprehension or prosecution of offenders
- assessment or collection of any tax or duty or of any imposition of a similar nature
- discharge of regulatory functions, including securing the health, safety and welfare of persons at work

Third party requests for personal data should be passed to the Data Protection Officer who, where appropriate, will authorise the release and format of data.

10. Rights to Access Information

Employees, students, Corporation members and other users of the College have rights to access personal data that is being held by the College in relation to them either on computer or in manual files.

All data subjects should be informed that they have the right to access their data. They should be told how they can exercise this right.

The fair processing statement, distributed at enrolment, advises learners that further information on how to access personal data may be obtained from the Data Protection Officer.

11. Requests for Information from Data Subjects (Subject Access Requests)

"Informal" Requests for Information

Subject to certain exemptions data subjects are entitled to request all the information that the College holds about them. However the majority of requests received by the College are likely to be from staff and students asking for copies of a specific document(s). These will usually be located in a single source, typically the Faculty staff/student files, and will not involve the disclosure of information relating to a third party.

In such cases, whilst the request will technically be a subject access request under the GDPR:

- College policy is to be open and transparent and wherever possible to let the individual have a copy of the information with minimum fuss.
- Requests should be handled directly by the relevant department or section.
- Ensure that you do not inadvertently release third party information without their consent.
- No fee will be charged.
- Requests do not necessarily have to be referred to the DPO, but it is important staff check with their line manager initially

“Formal” Requests

There may be some instances when a request for information is more complex.

Examples include:

- request involves locating information from multiple sources
- request involves the release of contentious information
- request is one in a series of requests from the same individual
- request involves the release of third party data for which consent has been refused or cannot be obtained
- the data subject does not want to ask for the information from the department/section that holds it.

In such cases, the request should be referred to the College Data Protection Officer who will ensure that a co-ordinated approach is adopted with relevant Data Owners. When responding to formal requests, the Data Protection Officer will liaise with staff in the department/section as appropriate.

Requests may be refused if they are deemed to be manifestly unfounded or excessive, or a fee could be applied.

In line with ICO guidance, a request may be manifestly unfounded if:

- The individual clearly has no intention to exercise their right of access; or
- The request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the individual:
- explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- makes unsubstantiated accusations against College employees which are clearly prompted by malice
- targets a particular employee against whom they have some personal grudge; or
- systematically sends different requests to the Controller as part of a campaign, e.g. once a week, with the intention of causing disruption.

To determine whether a request is manifestly excessive, the College will consider whether the request is clearly or obviously unreasonable, based on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request. This will mean taking into account all the circumstances of the request.

For manifestly unfounded or excessive requests a fee of £25 per hour for staff time/administrative costs, 5 pence per photocopied sheet, plus any additional postage charges will be applied.

The College may also seek legal advice if it is thought that requested information may be exempt or if disclosure would be unfair to any third party.

In line with GDPR, requests will be responded to within one month of receipt.

12. Requests for Information from Third Parties

Where employment agencies, prospective employers and similar bodies wish to request verification of details about a data subject, such as attendance records, examination results, and degree classifications, the request for the disclosure of the details to the third party should either **come from the data subject directly**, or the request from the third party should be **accompanied by a statement from the data subject** consenting to the disclosure.

Where the matter is **urgent**, an attempt should be made to contact the data subject by telephone or other means in order to put him or her in touch with the enquirer.

13. Disclosure of Student Data to Employers / Sponsors

Many students attend college under the sponsorship of their employers or other parties. This may include paid time to attend or payment of fees. These students will be asked to provide consent at enrolment that allow for the college to inform their employer of their progress, including attendance.

14. Students below the Age of 18

Parents and guardians of young people attending College below the age of 18 do not have automatic rights under the General Data Protection Regulation to information about their children. It is important to ensure appropriate communication between the home and the College.

Students below the age of 18 will be requested to consent to disclosing routine reports on academic progress and attendance as part of the application and enrolment process. GDPR guidance highlights that consent should be obtained from students aged 13 and above.

Other requests for information from parents or guardians should be considered carefully. It should be normal procedure to request permission from the student before disclosing any additional information.

15. Responsibilities of Contractors, Partners and Visitors

Visitors are often required to have access to areas in which personal data may be stored or processed. In certain circumstances, it may also be necessary, to allow certain visitors access to personal data in order to perform their contracted duties. Such visitors may include auditors appointed by the Funding Agencies and IT technicians employed by our software suppliers.

The College should ensure that all such visitors:-

- Sign in and are required to wear some form of identification
- Are not given unauthorised access to areas where personal data is held or processed
- Do not have access to personal data which is outside the scope of their appointed role
- Are aware of their responsibilities, under their contracted employment and GDPR, where access to personal data is unavoidable
- Have signed the College's Security Policy for Contractor's, Consultants and Suppliers

Further information is provided in the College's Security Policy for Contractor's, Consultants and Suppliers.

16. Transfers of personal data to non-EEA countries

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. The restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

The College will only transfer data outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

17. Medical Information

The College may ask staff and students about particular health needs, such as allergies to particular forms of medication, or other conditions such as asthma or diabetes.

The College will not use or share this information with third parties without explicit consent other than where this is necessary in exceptional circumstances (their 'vital interests') e.g. where required to do so by law or in the interests of an individual's health and safety and where the individual is not capable of giving their consent e.g. in a medical emergency.

18. Standard Student Data Collection & Processing

A large proportion of the personal information with which staff deal on a day to day basis in respect of students will be sensitive information, and will cover categories such as:-

- General personal details such as names and addresses
- Details about class attendance, course work marks and grades and associated comments
- Notes of personal supervision, including matters about behaviour and discipline

When collecting, processing and storing any kind of personal information, staff need to ensure that they comply with the Data Protection principles. In particular they must ensure that records are:-

- Collected and used fairly
- Accurate
- Up-to-date
- Stored securely
- Disposed of securely

Telephone Conversations and Meetings

If personal information is collected by telephone, callers should be advised what that information will be used for and what their rights are according to the General Data Protection Regulation.

Staff Checklist for Recording Students' Personal Data:-

- Do I really need this information about the student?
- Do I know what I'm going to use it for?
- Is the information "standard" or "sensitive"?
- Do I have the student's informed consent to process the information?
- If I do not have the student's consent to process, am I satisfied that the processing is nevertheless permitted by the DPA/GDPR?
- Am I sure the personal information is accurate and up to date?
- Have steps been taken to ensure that the data is stored securely?
- Once it is no longer needed, will the personal information be securely deleted or destroyed?

Examination results

Examination and assessment marks are covered by the GDPR. Staff should not release results to third parties without a signed authorisation of the data subject.

19. Training

The College will provide regular training to staff in respect of Data Protection. Refresher training will be required at least every three years or more often if required by any funding body or regulator (e.g. WBL).

20. Information Security

As a matter of policy, personal data of staff and students should be kept in as few locations as possible e.g. a student file, personnel file, Management Information System (QL). Personal information should not be printed off unnecessarily as this increases the likelihood of it being lost or accessed by an unauthorised person. Access should be restricted to those members of staff who have a legitimate reason for accessing it e.g. by using password protection in the case of electronic information, or lockable cupboards in the case of paper information.

Full details are contained in the College's Information Security Policy.

21. Retention of Records Containing Personal Data

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements. A table showing the retention time of a range of personal records is included as Appendix C of this policy. These times reflect current legislation and will be updated as necessary, if in doubt please contact the Data Protection Officer.

Weblogs will be retained by the Computer Services department for a period of 6 months.

Data may be destroyed only with the express permission of the relevant Data Owner.

Staff accounts: after a member of staff has left the College, accounts will be deleted after one year.

Student accounts: after College students have left the College, in the summer term, accounts will be retained for one term after leaving and deleted at Christmas.

22. Complaints

Data subjects who wish to complain to the College about how their personal information has been processed may use the College Complaints Procedure, or log their complaint directly with the College DPO who can be contacted at: dpo@gowercollegeswansea.ac.uk

Data subjects may also complain directly to the Information Commissioner's Office at: www.ico.org.uk

23. References & Sources

Information Commissioner's Office – **http://www.ico.org.uk**

Related College policies can be located at:
BIZ-Sharepoint/Intranet/Policies & Procedures/Data Protection

24. The Welsh Language

Mae Coleg Gŵyr Abertawe yn ymrwymedig i hyrwyddo'r iaith Gymraeg, yn unol â Safonau'r Iaith Gymraeg a Mesur y Gymraeg (Cymru) 2011.

Gower College Swansea is committed to the promotion of the Welsh language, in accordance with the Welsh Language Standards and the Welsh Language (Wales) Measure 2011.

APPENDIX A - Definitions

Data
Is recorded information that is processed on computer as well as any manual documents held by public authorities.

Data Subject
Is the person whose personal information is held by the College.

Subject Access Rights
Rights you have as a data subject to ask whether the College is holding personal data which relates to you and to be supplied with a copy of it.

Information Commissioner
The Information Commissioner's Office (ICO) is an independent body responsible for ensuring that organisations comply with the General Data protection Regulation (GDPR). It can take enforcement action in cases of breach of GDPR and can initiate prosecutions where offences have been committed. The ICO can also apply fines where breaches of GDPR have occurred.

The ICO also deals with complaints and enquiries about Data Protection.

Notification
The process by which the College notifies the ICO which types of personal information they hold and the purposes for which they process it. These details appear on a public Register of Data Controllers, which anyone can access.

The following are common terms which are referred to in the General Data Protection Regulation:

'**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in 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;

'**processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'**consent**' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'the right to be informed' encompasses the obligation to provide "fair processing information", typically through a privacy notice;

'the right of access' means under GDPR individuals have the right to confirm that their data is being processed, the right to access their personal data and the right to supplementary information as detailed in the privacy notice;

'the right to rectification' means under GDPR individuals have the right to have personal data rectified if it is inaccurate or incomplete;

'the right to erasure' means under GDPR individuals have the right to have to request the deletion or removal of their personal data where there is no compelling reason for its continued processing

'the right to restrict processing' can requested by an individual in certain circumstances;

'the right to data portability' allows individuals to obtain and reuse their personal data for their own purposes in a format suitable for their purposes.

'the right to object' allows individuals to object to the processing of their data in the public interest, object to direct marketing and object to processing for scientific, historical or statistical purposes.

'rights related to automated decision making and profiling' provides safeguards to individuals against the risk that a potentially damaging decision is taken without human intervention.

APPENDIX B - SUBJECT ACCESS/CORRECTION/DELETION/PORTING REQUEST

This form is to be completed by an individual who seeks access to personal data held about them by Gower College Swansea, or wishes to request correction, deletion, or porting of their personal data.

To help the College comply with your request please give accurate personal details and an indication of the details of your request.

The College will try to meet your request within one month of receipt of your request, but will contact you if we are not able to meet your request with the target timescale. In most cases there is no charge for a subject access request.

Current staff and students must produce their staff or student ID card for identification. Other requestors must provide copies of two items of **proof of identity** e.g. birth certificate, passport **must** be included.

SURNAME	FIRST NAME(s)	Date of Birth	GENDER

CURRENT ADDRESS:	ADDRESS: (at time at Gower College Swansea)

REQUEST: (please indicate)

STAFF ☐ **STUDENT** ☐ **OTHER** ☐

START DATE	FINISH DATE	SITE/LOCATION	COURSE TITLE/JOB TITLE

DESCRIPTION OF REQUEST:

I enclose proof of personal identity. ☐

Signed …… **Date** ……

Please return this form to the Data Protection Officer, Clerk to the Governors, Gower College Swansea, Tycoch Road, Swansea, SA2 9EB

For Office Use Only

Date Request Received : ……	Date of Data Supplied: ……

Notes:

Gower College Swansea – Data Access Request - CCTV

This form is to be completed by an individual who seeks access to personal data held about them by Gower College Swansea via its CCTV system.

To help the College comply with your request we will need information on the position of the camera and the date and time of the images you wish to access.

The College will try to provide the data you seek within one month of receipt of your request, but will contact you if we are not able to meet your request with the target timescale. In most cases there is no charge for a subject access request.

Current staff and students must produce their staff or student ID card for identification. Other requestors must provide copies of two items of proof of identity, at least one of which includes a **verified recent photograph** e.g. passport, driving licence, birth certificate must be included.

SURNAME	FIRST NAME(s)	Date of Birth	GENDER

CURRENT ADDRESS:	ADDRESS: (at time at Gower College Swansea)

REQUEST: (please indicate)

STAFF ☐ STUDENT ☐ OTHER ☐

DATE	Start time	Finish time	Camera location

DESCRIPTION OF DATA REQUIRED:

I enclose required proof of personal identity. ☐

Signed …… Date ……

Please return this form to the Data Protection Officer, Clerk to the Governors, Gower College Swansea, Tycoch Road, Swansea, SA2 9EB

For Office Use Only

Date Request Received : ……	Date of Data Supplied: ……

Notes:

APPENDIX C

Type of record	Retention period	Reason for length of period
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation.
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	6 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Limitation Act 1980
Wages and salary records	6 years from the end of the tax year	Taxes Management Act 1970
Income Tax and NI Returns, including correspondence with tax office	6 years from the end of the tax year	Income Tax (Employment) Regulation 1993 At least 3 years after the end of the financial year to which the records related
Statutory Maternity Pay records and calculations	6 years from the end of the tax year	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	6 years from the end of the tax year	Statutory Sick Pay (General) Regulations 1982
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	During employment	Management of Health and Safety at Work Regulations

Type of record	Retention period	Reason for length of period
Health Records where reason for termination of employment is connected with health, including stress related illness	6 years	Limitation period for personal injury claims
Medical records kept in relation to the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
FE Student data (required by Welsh Government)	10 years from the end of the academic year	Required by Welsh Government
WBL Student data (required by Welsh Government)	10 years from the end of the contract year	Required by Welsh Government
Student data/records (not required by Welsh Government), including academic achievements and conduct	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence	Limitation period for negligence.
	At least 10 years for personal and academic references.	Permits institution to provide references for a reasonable length of time.
	Certain personal data may be held in perpetuity.	While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data.

*** where documents relate to externally funded projects (eg ESF), original documents should be retained in accordance with the guidelines for that project. Please consult with the External Funding Manager before destroying documents, in particular student enrolment forms, wages and salary information.**

PROTOCOL FOR DEALING WITH REQUESTS FOR ACCESS/CORRECTION/DELETION OR PORTING OF PERSONAL DATA

1. Request received from individual or data controller.
2. Forward to DPO for review and forwarding to relevant parties.
3. DPO to forward request to data owner(s).
4. Data owner to progress request and respond to DPO.
5. DPO to respond to data subject.

Responses to requests must be made within one month. There is no charge for making these requests.