Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

UWTSD Group Data Protection Policy

Prifysgol Cymru
University of Wales

colegsirgâr

colegceredigion

Mae'r ddogfen hon ar gael yn Gymraeg ac yn Saesneg | This document is available in English and Welsh

Contents

1. Policy Statement

1.1 Everyone has rights about the way in which their personal data is handled. During the course of its activities the UWTSD Group and University of Wales will collect, store and process personal data about its staff, students, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation.

1.2 The policy covers, but is not limited to, systems developed or commissioned by UWTSD Group, any systems or data attached to UWTSD Group data or telephone networks, systems managed by UWTSD Group, mobile devices used to connect to the University networks or which hold University data, data over which UWTSD Group holds the intellectual property rights, data provided to 3rd party managed systems, including systems such as generative AI, data over which UWTSD is the data controller or data processor or electronic communications sent from UWTSD.

1.3 Data users are obliged to comply with this policy when processing personal data on the UWTSD Group's behalf. Any breach of this policy may result in disciplinary action.

2. About This Policy

2.1 The types of personal data that the UWTSD Group may be required to handle include, inter alia, information about current, past and prospective students and staff and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 ("the Act") as amended and the General Data Protection Regulation 2018 ("EU GDPR") see beneath.

2.2 The EU GDPR is the law that sets out the requirements for the protection of personal data within the EU. Following the UK's departure from the EU, from the 1st January 2021, the requirements of the EU GDPR were adopted into UK laws, creating the 'UK GDPR'. The EU GDPR will remain relevant to data collected and processed prior to the 31st December 2020 and to the data of EU residents from there on in. Data of UK residents, collected after the 1st January 2021 will be subject to the UK GDPR. As both the EU and UK versions of the GDPR are currently aligned, statements that refer to the 'GDPR' will serve to cover both regimes.

2.3 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time as required under the law.

2.5 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.6 The UWTSD Group Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is currently held by Paul Osborne foi@uwtsd.ac.uk . Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the UWTSD Group Data Protection Officer.

3. Definition Of Data Protection Terms

3.1 **Consent** is an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

3.2 **Data** is information which is stored electronically, on a computer, or in certain paper- based filing systems.

3.3 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.4 **Personal Data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.5 **Data Controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. UWTSD is the registered data controller for the purposes of this policy.

3.6 **Data Users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.7 **Data Processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the Group's behalf.

3.8 **Legitimate Interest** means the requirement to process personal data in order to carry out tasks related to our business activities for example: for direct marketing purposes, or the prevention of fraud.

3.9 **Personal Data Breach** is any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or

acquisition, of Personal Data is a Personal Data Breach.

3.10 **Privacy Notice**: Data protection laws require the Data Controller to provide detailed, specific information to the Data Subject about how and why their personal data is being processed (including the identity of the Data Controller and the Data Protection Officer, how and why the University will use, process, disclose, protect and retain that personal data). Such information must be provided through appropriate Privacy Notices.

3.11 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.12 **Special Category Data** is personal data revealing an individual's racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning physical or mental health (including disabilities) or sexual life or sexual orientation.

4. Data Protection Principles

4.1 Anyone processing personal data must comply with the following data protection principles. These provide that personal data must be:

4.1.1 Processed fairly and lawfully, and in a transparent manner.

4.1.2 Processed for limited purposes and in an appropriate way.

4.1.3 Adequate, relevant and not excessive for the purpose.

4.1.4 Accurate and that inaccurate data is rectified or deleted without delay.

4.1.5 Not kept longer than necessary for the purpose.

4.1.6 Processed in line with data subjects' rights and protected from accidental loss, destruction or damage.

4.1.7 Kept securely.

5. Fair And Lawful Processing

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the UK GDPR. These include, among other

things, the data subject's Consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When special category data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. Processing For Limited Purposes

6.1 In the course of our business, we may collect and process the personal data set out in a privacy notice. Privacy Notices must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub- contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for the specific purposes set out in the privacy notice for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. Notify Data Subjects

7.1 If we collect personal data directly from data subjects, we will inform them about:

7.1.1 The purpose or purposes for which we intend to process that personal data.

7.1.2 The types of third parties, if any, with which we will share or to which we will disclose that personal data.

7.1.3 The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.1.4 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.1.5 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the UWTSD Group Data Protection Officer is.

7.1.6 Privacy Notices should be provided at the point of collection of personal data and ideally via the same medium. The Data Subject should be notified of any change to a Privacy Notice. Given the level of engagement with external parties and industries and the range of initiatives with which

the group is involved, this may require regular review and management.

8. The Rights of Data Subjects

8.1 Individuals have a number of rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful;
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data; and
- obtain and reuse or have their personal data transmitted in a structured, commonly used and machine-readable format to another data controller.

8.2 To ask the UWTSD Group to take any of these steps, the individual should send the request to foi@uwtsd.ac.uk.

9. Legitimate Interests

9.1 The University may use your personal data where it is necessary to conduct our business and pursue our legitimate interests.

9.2 The University will always balance our legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account any particular circumstances.

9.3 We will not use your personal data for activities where our legitimate interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

10. Data Security

10.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Where the UWTSD Group Data Protection Officer considers there is a risk to the privacy of data subjects in relation to any proposed UWTSD Group policy, process or project then the UWTSD Group will carry out a data protection impact assessment which includes, inter alia, the purpose of the activity, risks and measures to be put in place to mitigate any potential/possible risks.

10.2 We will put in place procedures and technologies (including use of encryption and pseudonymisation) to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves and which are approved by the University Group's Data Protection Officer.

10.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

10.3.1 **Confidentiality** means that only people who are authorised to use the data can access it.

10.3.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

10.3.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the University's central computer system and the PCs of those employees authorised by senior managers ("authorised individuals") to have access to that information. In the exceptional event that it is necessary for authorised individuals to hold special category data and personal data on PCs, laptops, tablets or any other device outside of the University. All such data shall be encrypted.

10.4 Security procedures include:

10.4.1 **Entry controls:** Any stranger seen in entry-controlled areas should be reported to a Line Manager.

10.4.2 **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

10.4.3 **Methods of disposal:** Paper documents should be shredded or disposed of in accordance with the University's policy on confidential waste and the Record Management Policy. Digital storage devices should be physically destroyed when they are no longer required.

10.4.4 **Equipment:** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

10.5 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

10.6 We have put in place procedures to deal with any suspected Personal

Data Breach and will notify Data Subjects and/or the Information Commissioner where we are legally required to do so.

10.7 All breaches should be reported immediately to the UWTSD Group Data Protection Officer at foi@uwtsd.ac.uk. All evidence relating to the potential Personal Data Breach should be preserved to enable the UWTSD Group Data Protection Officer to carry out an investigation and report, where appropriate, to the Information Commissioner and Senior Leadership of the UWTSD Group.

11. Transferring Personal Data to A Country Outside The EEA

11.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

11.1.1 The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms as recognised as the UK Data Protection norm and UK GDPR.

11.1.2 The data subject has given his express consent to the transfer.

11.1.3 The transfer is necessary for one of the legal bases set out in UK GDPR, including, inter alia, the performance of a contract between the UWTSD Group and the data subject, or to protect the vital interests of the data subject.

11.1.4 The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

11.1.5 The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

11.2 Subject to the requirements in clause 10 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

12. Disclosure And Sharing of Personal Information

12.1 We may share personal data we hold with any member of the UWTSD Group. We may also disclose personal data we hold to third parties.

12.2 In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

12.3 If all or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

12.4 We may also disclose personal data or special category data if we are under a legal duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

12.5 We may also share personal data we hold with selected third parties but subject to the safeguards in this policy and in the UK GDPR.

13. Dealing With Subject Access Requests

13.1 Individuals have the right to access their personal data as held by the University by means of a subject access request.

13.1.1 Any individual who wishes to exercise this right can request access to their personal data either in writing or verbally. All applicants should complete the UWTSD Subject Access Request form and submit this to foi@uwtsd.ac.uk.

13.1.2 The requester must make it clear they are asking for their own information.

13.2 We will verify the identity of a data subject who requests access, for example: a passport or driving licence.

13.3 Any such subject access requests will be complied with within one calendar month of receipt of the request.

13.4 In exceptional circumstances and when necessary to respond to a complex request, or a number of requests from a data subject, it may be necessary to extend the response date by up to a further two months. In these circumstances we will inform the individual within one month of receiving their request.

14. Direct Marketing

14.1 We are subject to certain rules and privacy laws when marketing to our students, alumni and customers. A Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as a "soft opt-in" allows us to send marketing texts or emails to them if we have obtained contact details in the course of our relationship with them; that we are marketing similar products or services to them; and we have given them an opportunity to opt out of marketing emails from us when we initially collected their details and in every subsequent message we have sent to them.

15. Children

15.1 The following restrictions apply to the processing of personal information relating to children:

15.1.1 Online services offered directly to children require parental consent.

15.1.2 Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.

15.1.3 The use of child data for marketing or for profiling requires specific protection.

The Data Protection Officer should be informed if any of the above activities are being contemplated.

16. Record of Processing Activity

16.1 The University holds a record of processing activity ("ROPA") which records the way the University processes personal data of its students and staff. The ROPA is available at Data Protection | University of Wales Trinity Saint David (uwtsd.ac.uk).

17. Changes To This Policy

17.1 The UWTSD Group and University of Wales reserves the right to change this policy at any time with the approval of the Senior Leadership Team. Where appropriate, we will notify data subjects of those changes by mail or email.

Document Version Control

Version No:	Reason for change:	Author:	Date of change:
1.1	Policy Review Update	PO	02.04.20
1.2	Policy Review Update	PO	08.10.21
	Considered at OLT and APT – 02.11.21.		
1.3	Policy review and updated	PO	16.04.24
1.4	Policy approved by SLT – 5th November 2024		

(This should include the journey of the policy through the Committee structure).

Policy author(s): Paul Osborne **Job Title: UWTSD Group DPO**

Current status of Policy: approved
Is the Policy applicable to: Both FE and HE

Date effective from: 05 / 11 / 2024

Policy review date: 16 / 04 / 2024

Policy reviewed and updated: 05 / 11 / 2024 (approval by SLT)

Next review due: 04 / 11 / 2025

For publication: on FE and HE Websites / FE and HE Intranets

Approval
The policy will be formally considered and approved in accordance with Committee Terms of Reference outlined in the Academic Quality Handbook.

If the policy affects staff, advice should be sought from HR at the outset to ascertain if consultation is required at JCC. HR will also provide advice on the most appropriate stage to consult with JCC and on whether approval by Council is required.

ALL policies submitted for approval must be accompanied by a completed:

- ***Equality and Welsh Language Impact Assessment***
- ***Institutional Impact Assessment Privacy Impact Assessment***

Prior to submission to committee, authors are asked to consult the Policy and Planning Team who will check that the document complies with University requirements. The Policy and Planning Team will complete the section below.

For completion by the Policy and Planning Team

Please tick to confirm the following:

An institutional Impact Assessment has been completed ☒

An Equality and Welsh Language Impact Assessment has been completed ☒

A PIA has been completed ☒
Matters requiring consideration by the approving committee: None

---

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David