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

coleg ceredigion

coleg sirgâr

UWTSD Group Data Protection Policy

Contents

1. Policy statement 3
2. About this policy 3
3. Definition of data protection terms 3
4. Data protection principles 4
5. Fair and lawful processing 5
6. Processing for limited purposes 5
7. Notifying data subjects 5
8. The rights of data subjects 5
9. Data security 6
10. Transferring personal data to a country outside the EEA 7
11. Disclosure and sharing of personal information 7
12. Dealing with subject access requests 8
13. Direct marketing 9
14. Changes to this policy. 9

1. Policy statement

Everyone has rights with regard to the way in which their personal data is handled. During the course of its activities the UWTSD Group 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.

Data users are obliged to comply with this policy when processing personal data on its behalf. Any breach of this policy may result in disciplinary action.

2. About this policy

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 (GDPR).

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.

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.

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

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

Consent: 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.

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

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.

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.

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. The UWTSD Group Data Protection Officer is the data controller of all personal data used in our business for our own commercial purposes.

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.

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 University's behalf.

Personal Data Breach: 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.

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.

Special Category Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special Category Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. Data protection principles

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

4.1 Processed fairly and lawfully, and in a transparent manner
4.2 Processed for limited purposes and in an appropriate way.
4.3 Adequate, relevant and not excessive for the purpose.
4.4 Accurate and that inaccurate data is rectified or deleted without delay
4.5 Not kept longer than necessary for the purpose.
4.6 Processed in line with data subjects' rights and protected from accidental loss, destruction or damage.
4.7 Is 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 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. Notifying data subjects

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

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

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

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

7.5 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.

7.6 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.

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; and
- 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.

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

9. Data security

9.1 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.

9.2 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 she/he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself and which are approved by the University Group's Data Protection Officer.

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

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

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

9.6 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

9.7 Security procedures include:

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

9.7.2 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.)

9.7.3 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.

9.7.4 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.

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

9.9 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.

9.10 All breaches should be reported immediately to the UWTSD Group Data Protection Officer at foi@uwtsd.ac.uk You should preserve all evidence relating to the potential Personal Data Breach to enable the UWTSD Group Data Protection Officer to carry out his investigation and report to the Information Commissioner and Senior Management of the UWTSD Group.

10. Transferring personal data to a country outside the EEA

10.1 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:

10.1.1 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 GDPR

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

10.1.3 The transfer is necessary for one of the legal bases set out in 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.

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

10.1.5 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.

10.2 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.

11. Disclosure and sharing of personal information

11.1 We may share personal data we hold with any member of the UWTSD Group.

11.2 We may also disclose personal data we hold to third parties:

11.3 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.

11.4 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.

11.5 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.

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

12. Dealing with subject access requests

12.1 Data subjects may make a formal request for information we hold about them (a subject access request). This must be made in writing. Employees who receive a written request should forward it to the UWTSD Group Data Protection Officer at foi@uwtsd.ac.uk immediately.

12.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

12.2.1 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

12.2.2 We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

12.3 In the event of any doubt or difficult, non-routine enquiries, matters must be referred to the UWTSD Group Data Protection Officer.

13. Direct marketing

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 you if we have obtained contact details in the course of our relationship with you ; that we are marketing similar products or services to you; and we have given you an opportunity to opt out of marketing emails from us when we initially collected your details and in every subsequent message we have sent to you.

14. Changes to this policy.

The UWTSD Group reserves the right to change this policy at any time with the approval of the relevant Committee. 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

(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: 24 / 05 / 2018

Policy review date: 1 / 12 / 2018

Policy reviewed and updated: 02/04/2020

Next review due: 03/04/2021

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 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 EIA has been completed ☒

A PIA has been completed ☒

Matters requiring consideration by the approving committee: None

---