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

colegsirgâr

colegceredigion

# Group Policy on taking sensitive information and personal data outside of the secure computing environment

# CONTENTS

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

## 1. Purpose

This document sets out policy on the storage, transmission and use of personal data and sensitive business information outside the University / College. This includes data on mobile devices and portable storage media. The policy relates to the University of Wales Trinity Saint David (UWTSD), and its constituent colleges, Coleg Sir Gâr and Coleg Ceredigion, referred to as the UWTSD Group.

This policy applies to all staff who store, transmit and use personal data and sensitive business information outside the University / College, including, but not limited to, the use of mobile devices (e.g. laptops and mobile phones), portable storage media (e.g. memory sticks or CDs) or other forms of communication (e.g. email). This policy is to be read in conjunction with the Mobile Phone Policy.

This policy relates to storage, transmission and use of personal data and sensitive business information on University / College owned mobile storage devices and personally owned mobile storage devices.

## 2. Background

The General Data Protection Regulation 2016 (GDPR) and The Data Protection Act 2018 set out, inter alia, how organisations may use personal data. The legislation states, "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

This requirement involves a judgement as to what measures are appropriate in particular circumstances. This policy provides guidance for staff on how to make this judgement when using, transporting or storing personal data or highly sensitive information outside the University / College.

## 3. Scope

The definition of "personal data" is complex, but for day-to-day purposes it is advisable to treat all information about living, identifiable individuals as "personal data".

The “personal data or sensitive business information” section below gives examples of personal data and sensitive business information. This list is for illustration only, is not exhaustive and may change from time to time.

For the purposes of this policy, personal data and sensitive business information might be in a variety of formats, including but not limited to email, word processed documents, spreadsheets and databases.

Information is considered to be "outside the University / College" if it is stored on a mobile device, transmitted by email or otherwise stored on a system that is not managed by or provided under contract to the University / College.

"A mobile device" is defined as any transportable device that is capable of storing data. This definition covers a wide range of equipment, from the basic USB memory stick or memory

card, pocket memo devices and laptops. It also includes i-Pods, MP3 players, digital cameras, camcorders, audio recorders, CD/DVD, PDA, tablets, Blackberries, smartphones, iPads, iPhones and other external hard drives and devices.

## 4. Policy statement

All data or sensitive business information (as specified in the "personal data or sensitive business information" section beneath) must be encrypted if it leaves the University / College environment.

## 5. Key principles

The following key principles underpin this policy on the storage, transmission and use of personal data and sensitive business information. All staff must comply with these principles when using mobile devices and portable storage media or otherwise removing information outside the University/College:

i. Avoid using personal data wherever possible.

ii. If the use of personal data is unavoidable, consider partially or fully anonymising the information to obscure the identity of the individuals concerned.

iii. Use the University / College secure shared drives to store and access personal data and sensitive business information, ensuring that only those who need to use this information have access to it.

iv. Use remote access facilities to access personal data and sensitive business information whenever possible instead of transporting it on mobile devices or using third party hosting services.

v. If there is no option but to use mobile devices or email for personal data or sensitive business information, use encrypted memory sticks, or consult IT Service Desk in the use of encryption software.

vi. Do not use personal equipment (such as home PCs or personal USB sticks) or third party hosting services (such as Google Mail) for personal data or sensitive business information.

vii. Avoid sending personal data or sensitive business information by email. If you must use email to send this sort of data outside the University / College, it must be encrypted. If you are sending unencrypted personal data or sensitive business information to another person within the UWTSD Group via email, indicate in the email title that the email contains sensitive information so that the recipient can exercise caution when opening it.

viii. Do not consider and/or display personal data or sensitive business information in public places. When accessing email remotely, exercise caution to ensure that unencrypted personal data or sensitive business information or data is not downloaded to an insecure device.

ix. Consider the physical security of personal data or sensitive business information, for example, use locked filing cabinets/cupboards for storage.

x. Implement the University / College Records Retention Policy so that personal data and sensitive business information are kept for no longer than is necessary.

## 6. Personal data or sensitive business information

The following are examples of personal data or sensitive business information falling within the remit of this policy (this list is for information only, is not exhaustive and may change from time to time):

i. Any set of data relating to identifiable individuals, including, but not limited to students, staff, alumni and research participants.

ii. Any set of data relating to identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary.

iii. Information relating to individuals' performance, grading, promotion or personal and family lives.

iv. Information relating to alumni or students' programmes of study, grades, progression, or personal and family lives.

v. Any set of data relating to an identifiable individual's health, disability, ethnicity, sex life, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence.

vi. Health records of any identifiable individual.

vii. Substantial re-organisation or restructuring proposals that will have a significant impact on individuals before the decision is announced.

viii. Discussion papers and options relating to proposed changes to high profile strategies, policies and procedures, such as the admissions policy, before the changes are announced.

ix. Security arrangements for high profile or vulnerable visitors, students, events or buildings while the arrangements are still relevant. This includes door access codes and passwords for access to the network or other key systems.

x. Exam questions before the exam takes place.

xi. Non-public data that has the potential to seriously affect any organisation's commercial interests or the reputation of the UWTSD Group.

xii. Information obtained under a confidentiality agreement where disclosure of the information is likely to seriously affect the UWTSD Group's reputation or lead to an action against the UWTSD Group for breach of confidence.

xiii. Information that, if compromised, would substantially disadvantage the UWTSD Group in commercial or policy negotiations.

xiv. No personal data or sensitive business information may be uploaded to any "Cloud" environment other than those used by the UWTSD Group or which has been authorised by the University's Executive Head of IT & S.

## 7. Consequences of non-compliance

Failure to comply with this policy could expose the UWTSD Group, its staff or students to risks including fraud, identity theft and distress, or damage the UWTSD Group's reputation and its relationship with its stakeholders, including research funders. Any individual who breaches this policy may be subject to disciplinary action at the discretion of the Vice Chancellor (and/or his nominee) or the College Principal.

The Information Commissioner can also levy a fine on the UWTSD Group or on an individual for a breach of GDPR and / or the Data Protection Act 2018.What help is available?

## 8. What help is available?

Guidance on encryption is available via the IT Service Desk in the University and College.

The Data Protection and Records Section provides advice, guidance and training on data protection, records management and freedom of information issues. You can contact the Section by email:

foi@uwtsd.ac.uk or the University's Data Protection Officer paul.osborne@uwtsd.ac.uk or the College data protection officer dataprotectionofficer@colegsirgar.ac.uk

## 9. Resource Implications

| Implication | Detail |
|---|---|
| Finance | No additional costs have been identified. |
| Staff | No additional resource requirements have been identified. |
| Assets | No additional asset requirements have been identified. |
| Partners | None identified. |
| Timescales | This policy will come into immediate effect upon its approval. |
| Leadership | APVC Corporate and Quality. |

## 10. Impact Assessment

| Implication | Impact Considered (Yes/No) | Impact Identified |
|---|---|---|
| Legal | Y | The Policy supports University compliance with the Data Protection Act 1998. |
| Contribution to the Strategic Plan | Y | The policy supports the University's Strategic Plan, its mission, vision and values and is particularly aimed at promoting equality of access and opportunity. |
| Risk Analysis | Y | The Policy aims to manage the risk of personal data being inappropriately used, stored or shared. |
| Equality | Y | The policy aims to protect personal data thereby promoting equality of opportunity to all. |
| Welsh Language | Y | The policy is equally applicable to data stored and shared in the medium of Welsh. Advice and guidance on whether information shared through the medium of Welsh is sensitive can be sought from the University's Data Protection Officer. |
| Environmental and Sustainability | Y | The Policy promotes and supports sustainability through the application of appropriate storage and retention of personal and sensitive data. |
| Communication/ Media / Marketing | Y | The Policy will be available to access on the UWTSD website. See Strategies and Policies. Page. |

**Policy author(s):**

Paul Osborne – Data Protection Officer.

## 11. Document version control

| Version No: | Reason for change: | Author: | Date of change: |
|---|---|---|---|
| 1.0 | Initial Draft Policy for submission to SMT. | PO | |
| 1.1 | Update of policy to be applicable to the UWTSD Group. | CG | 30.05.18 |
| | | | |
| | | | |

**Current status of Policy**: Draft

**Is the Policy applicable to:** FE / HE

**Date ratified**: day / month / year**

**Date effective from**: day / month / year**

**Policy review date**: day / month / year**

**For publication:** on UWTSD website.

*Delete as appropriate
** insert when available