Privacy and Data Protection Notice – Employee Data

**Introduction**

1. Aberystwyth University (AU) is the Data Controller and is committed to protecting the rights of employees in line with the UK Data Protection Act (DPA) and the General Data Protection Regulation (GDPR) introduced in 2018.

1. The contact address of the Data Controller is:

Aberystwyth University

Reception

Penglais Campus

Aberystwyth

Ceredigion

SY23 3FL

**Why does the University process personal data?**

1. The University needs to process personal data (information) about employees so that it can:

*(i) undertake administration of prospective, current and past employees including self-employed, contract personnel, temporary staff or voluntary workers;*

*(ii) administer recruitment and selection processes;*

1. *undertake administration of non-University staff contracted to provide services on behalf of the University;*
2. *plan and manage the University’s workload or business activity;*
3. *provide an occupational health service;*
4. *undertake the administration of agents or other intermediaries;*
5. *manage pensions administration;*
6. *manage case work including disciplinary matters, staff disputes, employment tribunals;*
7. *organise staff training and development;*
8. *ensure that staff are appropriately supported in their roles;*
9. *undertake vetting checks;*
10. *assess the University’s performance against equality objectives as set out by the Equality Act 2010.*

**What data is processed?**

4.The Universitymay need to process a wide range of data relating to employees. Classes of data may include:

4.1 Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses

4.2 Date of birth

4.3 Gender

4.4 Marital status and dependants

4.5 Next of kin and emergency contact information

4.6 National Insurance number

4.7 Bank account details, payroll records and tax status information

4.8 Salary, annual leave, pension and benefits information

4.9 Start date

4.10 Location of employment or workplace

4.11 Copy of driving licence

4.12 Copy of passport and, where relevant, visa and right to work documentation

4.13 Recruitment information (including copies of right to work documentation, details of your experience, education and training, references and other information included in a CV or cover letter or as part of the application process, and/or confirmation that you have satisfied a Disclosure and Barring Service enquiry, if required for the role)

4.14 Employment records (including job titles, work history, working hours, training records and professional memberships)

4.15 Salary, benefits and compensation history

4.16 Details about your role(s) in the University, including any information relating to your undertaking of such role(s) (for example copies of performance information including Performance and Development Reviews, sickness records)

4.17 Disciplinary and grievance information

4.18 CCTV footage and other information obtained through electronic means such as swipecard records

4.19 Information about your use of our information and communications systems.

4.20 Photographs

4.21 Information about your use of the academic and non-academic facilities and services that we offer

4.22 A Register of Interests, covering all academic staff and any support staff, who have relevant interests to disclose. Where relevant, we may supplement these records with personal data from the public domain (e .g. your publications) or other sources

5. Some of the information processed may be defined as sensitive or, more specifically, classified as

‘special category data’ under the GDPR) , i.e.

*racial or ethnic origin; political opinions;*

*religious beliefs or other beliefs of a similar nature;*

*membership of a trade union;*

*physical or mental health or condition;*

*sexual life;*

*genetics;*

*and unique identity as processed by biometric data.*

The University may also need to process information regarding criminal convictions particularly where DBS checks are undertaken in relation to particular roles.

**Legal basis for processing**

1. Staff personal data is processed because it is necessary for the performance of the contract between staff members and the University or in order to take steps to enter into that contract (GDPR 6 (1) (b)).

 Some of that data is also processed because of specific legal obligations such as those dictated by health and safety legislation and the requirements for reporting to i) UK Visas and Immigration and ii) the Higher

Education Statistics Agency (GDPR 6 (1) (c)).

There may also be circumstances where further information is requested from you, such as insurance details in relation to travel arrangements or driving whilst in the performance of University business. In these cases, the information will be processed as it is in the legitimate interests of the University as data controller.

1. Some information will be retained after your period of employment as a member of staff in line with legal requirements and also to continue pensions administration. There may be circumstances whereby the University may need to contact staff after they have left in relation to these purposes.

**Access to, sharing and disclosing employee data**

1. Staff contact details will normally be publicly available via the University Directory. This will include name, job title, department, work address, email address and telephone number. There are some circumstances where certain details may be omitted on request. Further information, such as CVs, photos and research interests, may also be made available on the departmental/institute websites, where relevant, to promote the University’s work and that of individual members of the academic staff. This may be automatic in the case of academic members of staff in order to facilitate contact by students and external parties, but in the case of non-academic members of staff (with the exception of front-facing staff as described below) this should only take place with the consent of that member of staff. Staff involved in research may also have their contact details and information relating to their areas of research shared on a variety of platforms, some of which are provided by third parties.

1. Staff working in customer or ‘front-facing’ positions may be expected to wear name badges as appropriate, and may also have their names displayed on till receipts. Names and photographs may also be displayed on noticeboards.

1. Day-to-day personal data (e.g. contact data, attendance and payment information) relating to staff will normally be accessible to staff working in Human Resources and to line managers, senior managers and administrators within the relevant department. Sensitive (‘special category’) personal data will only be shared internally in more limited circumstances such as where there is a legitimate business need, obligation, or legal duty, such as details of a disability. Sensitive data may also be shared with individuals contracted to provide support for staff, such as occupational health specialists. In relation to particular processes, such as investigations or appeal panels, other senior University staff and members of University Council may be given access to personal data, including sensitive categories of data.

1. The University’s email and calendar service is provided by Microsoft. The contents of email and calendar accounts are therefore held by this third party in accordance with data protection legislation. The University has a written contract in place to ensure the protection of University-owned personal data.

12. The University operates a CCTV system around its sites, the purpose of which is to create a safer environment for students, employees and visitors to the University. Due to the nature of such a system it is likely to capture images of employees on a frequent basis. CCTV is limited to ‘public areas’, locations regularly used by employees and students and thoroughfares and is not used for the routine monitoring of staff. Images are only used in circumstances that could not be reasonably ignored by the University, such as where there is a risk of, or actual, criminal activity taking place, where there is alleged gross misconduct or where the behaviour of employees may put others at risk. Where images are used in any disciplinary procedures the individual member of staff will have access to the relevant CCTV footage.

13. The University will make some statutory and routine disclosures of personal data to third parties where appropriate. These third parties include:

* 1. Higher Education Statistics Agency (HESA). For details see: <https://www.hesa.ac.uk/about/regulation/data-protection/notices> and <https://www.aber.ac.uk/en/hr/policy-and-procedure/hesa/>
	2. UK Visas and Immigration
	3. HM Revenue and Customs (HMRC)
	4. Pension schemes – including USS and others (as set out in the scheme rules)
	5. Research sponsors, funding bodies and contracted agencies working on behalf of these bodies
	6. Trade unions
	7. Potential employers (where a reference is requested)
	8. Benefits Agency as required by the Social Security Administration Act 1992
	9. Child Support Agency/Child Maintenance Service as required by the Child Support Information Regulations 2008 (no.2551)
	10. Higher Education Funding Council for Wales
	11. Auditors, insurers and solicitors acting for the University or for government bodies
	12. Professional bodies (e.g. The Law Society) - where this is necessary for course accreditation and/or the performance of contractual duties

(xii) Other organisations with which the University is collaborating on research projects

14. Personal data may be released under the Freedom of Information Act 2000 where disclosures do not breach the data protection legislation.

15. Personal data may also be disclosed when legally required, or where there is a legitimate interest, or when requested by the police or security services, including under the ‘Prevent’ duties placed on the University by the Counter-Terrorism and Security Act 2015 .

1. The University may use third party companies as data processors to carry out certain administrative functions on behalf of the University. When this occurs, a written contract will be put in place to ensure that any personal data disclosed to that third party company will be held in accordance with data protection legislation. Some of these processes (e.g. travel arrangements and booking) may involve staff providing personal data directly to third party service providers.

1. The University will usually only share your personal data with third parties outside of the EU if you have given your consent. However, there may be circumstances where information is shared without consent. This will only be if:
	* 1. The EU has concluded that the third country has an adequate level of protection
		2. The disclosure is to a US company which has signed up to the Privacy Shield principles
		3. It is necessary to protect your vital interests; for example in situations of medical emergency
		4. It is necessary for the performance of a contract between you and the University
		5. It is necessary for the purpose of obtaining legal advice or for the purposes of any legal proceedings

1. The University retains personal data (including that relating to employees) in line with its established retention schedules and with the model retention schedules established by the Joint Information Systems Committee (JISC).

**Data Subject Rights**

1. Under current data protection legislation an individual has the right to a copy of personal information held on them by the University and a right to raise an objection to data processing that causes unwarranted and substantial damage and distress.

It should be noted that although an objection can be made, in some circumstances the University may be required to hold certain information in order to carry out its legitimate business and to comply with specific sections of the DPA or GDPR. To discuss any objections or concerns, individuals should contact the Data Protection Officer at the e-mail address provided below.

1. Further information regarding the rights of data subjects can be found here: <https://www.aber.ac.uk/en/infocompliance/policies/dp/data-subject-rights/>and more information is available from the Information Commissioner’s Office ([https://ico.org.uk/)](https://ico.org.uk/). If you have any questions regarding the processing of staff personal data at the University, please contact the Data Protection Officer at infocompliance@aber.ac.uk

**Last amended July 2019. Due for review July 2020.**