Data Protection Policy

Rev	Date	Purpose of Issue/Description of Change	Equality Impact Assessment Completed
1.	November 2005	Initial Issue	
2.	5th October 2009	Revised and updated	
3.	15th June 2012	Revised and approved by the Legal Compliance Task Group	
4.	5th October 2015	Reviewed and approved by the Compliance Task Group	1st December, 2015
5.	3rd October 2016	Reviewed and approved by the Compliance Task Group	
6.	16th July 2018	Reviewed and approved by the Compliance Task Group	
7.	1st June 2020	Revised and reapproved by the Compliance Task Group	

Policy Officer	Senior Responsible Officer	Approved By	Date
Head of Governance and Compliance	University Secretary	Compliance Task Group	1st June 2020

This policy will be reviewed in 3 years

DATA PROTECTION POLICY

Bangor University takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (the Act) very seriously. This document provides the policy framework through which this effective management can be achieved and audited.

1. Purpose & Scope

The purpose of this policy is to ensure that the University and the University's staff and students comply with the provisions of the GDPR and the Act and with any other relevant legislation in jurisdictions in which the University operates when processing personal data. Any infringement of the Act will be treated seriously by the University and may be considered under disciplinary procedures.

This policy applies to staff, students, agents of the University and any authorised processors of personal data held or owned by the University, regardless of where the data is held and, in respect of automatically processed data, the ownership of the equipment used, if the processing is for University purposes. This policy also applies to personal data retained and processed by Bangor University Students' Union.

2. Data Protection Definitions

2.1 Personal data

Personal data is information that either on its own, or when combined with other information, can identify a living individual. This can include (but is not limited to):

Names, addresses, student and staff ID numbers, dates of birth, photographs, social media handles, video footage and emails.

The main types of personal data that the University uses are: Staff Data, Student Data (prospective, current and alumni) and Research Data.

2.2 Special Category Data

Special category data is personal data that needs more protection because it is sensitive. The GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

2.3 Processing

Data protection legislation refers to the processing of personal data. Processing simply means any use of personal data. This can range from collecting it to sharing it, from amending it to deleting it. The University needs to process information about its employees, its students and other individuals: for example, to allow it to

monitor performance, achievements and health and safety, and so that staff can be recruited and paid, courses organised and legal obligations (e.g. to funding bodies and the government) fulfilled. Such information must be collected and used fairly, stored safely and not disclosed unlawfully.

3. The Principles of Data Protection

The University is required to adhere to the principles of data protection as laid down by the Act. In accordance with those principles personal data shall be:

1. Processed fairly, lawfully and in a transparent manner
The University must be open and clear about what the personal data will be used for and how it will be used.

2. Processed for specified, explicit and legitimate purposes
The University must ensure that it collects personal data for clear, appropriate and legitimate purposes. Collecting personal data "just in case" for future reference is not compliant with legislation.

3. Adequate, relevant and limited to what is necessary for the purposes for which they are processed
The University must only collect, use or share personal data in a proportionate way. This means that it should collect what it needs to complete its purposes.

4. Accurate and up to date
Personal data must be accurate and up to date. Collecting inaccurate data is a breach of GDPR.

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Personal data must only be kept for a specific period of time. This time period will vary depending on what purpose the personal data is collected for - the University's Record & Data Retention Schedule details how long personal data should be kept for each function.

6. Processed in a manner that ensures appropriate security of the personal data
The University is required to have appropriate technical and organisational measures in place to ensure the security of personal data. This is applicable to both data held electronically and personal data within physical documents.

4. The Rights of the Individual

In addition to the data processing principles, the GDPR also sets out a range of rights individuals can use to understand how their personal data is used or exert an amount of control over how it is used. The rights include:

The right to be informed
An individual has the right to be informed about the collection and use of their personal data.

The right to access (often called Subject Access Requests)
An individual has a right to see a copy of the personal data held about them by the University and find out what it is used for. See 6.1 below for further details.

The right of rectification
An individual can request that inaccurate information held about them is either rectified or deleted.

The right to erasure (also known as the right to be forgotten)
An individual may ask for their personal data to be deleted by the University.

The right to restrict processing
An individual has the right to request the restriction of suppression of their personal data (i.e. whilst a complaint is being dealt with the University can store the personal data, but not use it).

The right to data portability
Allows individuals to obtain and reuse their personal data for their own purposes across different organisations.

The right to object
An individual has the right to object to the processing of their personal data, for instance to stop their data being used for direct marketing.

Rights related to automated decision-making including profiling
An individual has the right to stop automated decisions being made about them and ask for human intervention instead.

5. Responsibilities

[a] University Responsibilities

The University is a data controller under the Act and under equivalent legislation in other jurisdictions. The University is responsible for establishing policies and procedures and providing access to training in order to comply with the requirements of the Act.

[i] The Compliance Task Group

The Compliance Task Group is responsible for the development, implementation, monitoring and review of the University's Data Protection Policy and associated Procedures. The Compliance Task Group is chaired by the University Secretary and reports to the University Executive who are ultimately responsible for overseeing compliance in this area.

[ii] University's Data Protection Officer

- The Compliance Task Group will nominate an appropriate person as the University's Data Protection Officer, who will be a person of sufficient knowledge and seniority in the University.
- The nominated University Data Protection Officer is the Head of Governance and Compliance in the Governance and Compliance Office.
- Bangor University has notified the Information Commissioner's Office that it processes personal data, and queries relating to the University's notification should be directed to the Data Protection Officer.
- The University will make arrangements for the identity of the University's Data Protection Officer to be made known to all staff, students, consultants, contractors and volunteers and will also draw to their attention this Policy and associated documentation.
- The Data Protection Officer is tasked with drawing up guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information.
- The Data Protection Officer (or nominee) has access to all relevant documents relating to a legal compliance request and it is the Data Protection Officer (in consultation with the relevant senior officers) that will make the decisions regarding what information is released or exempted.

[b] Responsibilities of Pro Vice-Chancellors / Heads of College, Heads of School and Directors of Professional Services

Pro Vice-Chancellors / Heads of College, Heads of School and Directors of Professional Services are responsible for ensuring compliance with legislation in relation to personal data and for ensuring that the requirements of this Policy are met.

Pro Vice-Chancellors / Heads of College, Heads of School and Directors of Professional Services may choose to delegate the management of, but not the responsibility for, Data Protection matters to a school or departmental Data Protection Co-ordinator. This person will administer and co-ordinate the processes set up within the College, School or Department to manage compliance with data protection legislation and the University's guidance in this area, and will be a knowledgeable and accessible point of contact for people within the College, School or Department who have questions about data protection issues. Where a Dean, Head or Director chooses to delegate the management of data protection within their College, School or Department the University will provide data protection training which the Data Protection Co-ordinator will be required to undertake.

Responsibility for compliance with the Act's requirements with regard to personal data on Bangor University alumni has been delegated to the Executive Director of Development & Alumni Services (DAS). Heads of Schools holding and using information on alumni must keep DAS informed about all activities involving former students.

As part of its internal and external audit programme the University will perform periodic audits to ensure compliance with this Policy and the Act and to ensure that the notification is kept up to date.

Pro Vice-Chancellors / Heads of College, Heads of School and Directors of Central Service Departments must ensure that all new members of staff receive an introductory briefing on the Act and that relevant staff members within their areas of responsibility (those dealing with personal and / or sensitive personal data), including any relevant consultants / contractors, receive refresher courses on data protection compliance (available by contacting the Staff Development Unit, Human Resources).

[c] Staff Responsibilities

[i] When staff members use personal information about students, other members of staff or other individuals they must comply with the requirements of this Policy.

[ii] It is a condition of employment that staff will abide by the rules and policies of the University. Any failure to follow this Policy may result in disciplinary proceedings.

Staff must ensure that:

- all personal information entrusted to them in the course of their employment is kept securely.
- no personal information is disclosed either verbally or in writing, accidentally or otherwise to any unauthorised third party.
- no personal information should be accessed by staff for any reason other than for legitimate University business.
- any information that they provide to the University in connection with their own employment is accurate and up to date and that they inform the University of any changes, e.g. changes of address.

[iii] When members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection Principles as set out in point 3. above, in particular, the requirement to obtain the data subject's freely given, specified, informed and unambiguous consent where appropriate.

A Bangor University student should only use personal data, in relation to their studies, with the knowledge, written agreement and supervision of an appropriate member of staff. This would normally be a postgraduate student's supervisor, or for an undergraduate student the member of staff responsible for teaching the module. Consideration should also be given to the requirements of the University's Research Ethics Policy in relation to the use of personal data in research.

[iv] Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from their line manager or the Head of Governance and Compliance.

[d] Contractors, Short-Term, Casual and Voluntary Staff

The University is responsible for the use made of personal data by anyone working on its behalf. Pro Vice-Chancellors / Heads of College, Heads of School and Directors of Professional Services who employ contractors, short term, casual or voluntary staff must ensure that:

- Any personal and / or special category data collected or processed in the course of work undertaken for the University, is kept securely and confidentially. This applies whether the data is an integral part of the work, or whether it is simply contained on media or in places which contractors etc. need to access; it applies whether or not the University explicitly mentions the data in the contract.
- All personal and / or special category data is returned to the University on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and the University receives notification in this regard from the contractor or short term / voluntary member of staff.
- The University receives details of any disclosure of personal and / or special category data to any other organisation or any person who is not a direct employee of the contractor.
- Any personal and / or special category data made available by the University, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the Head of Governance and Compliance at the University.
- All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.
- The University's standard data protection clause must be inserted into all relevant University contracts.

6. Detailed Policy Requirements

6..1. Subject Access Requests

An individual is entitled to receive from the University:

- Confirmation as to whether or not personal data concerning them is being processed, and

- Where that is the case access to the personal data, and information relating to the purpose of the processing, the categories of personal data being processed, the recipients to whom the personal data has been disclosed, the retention period for the data and the complaints process.

Individuals wishing to access their own personal data held by the University can do so via a Subject Access Request. Any individual wishing to exercise this right should do so in writing or by email (info-compliance@bangor.ac.uk) to the Head of Governance and Compliance. A standard form is available on the University's data protection web pages.

Individuals will not be entitled to access information to which any of the exemptions in the Act applies. However, only those specific pieces of information to which the exemption applies will be withheld, and information covered by an exemption will be subject to review by the Head of Governance and Compliance

The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month as stipulated by the Act and within any relevant time periods set by other jurisdictions.

Requests for access to information held by the University's Student Counselling service will be dealt with by the Head of Governance and Compliance in consultation with the Head of Counselling.

6.2 Consent to process

It is a condition of the registration of students, and of the employment of staff, that individuals agree to Bangor University's processing of specified classes of personal data, including special category data. The University relies on a variety of legal grounds to process information, this includes information required under contract, information which is collected under public task, and information which the University believes it has legitimate interest to process. In some cases, the University needs to process information that, by the definition set out in the GDPR, is classed as special category data. Such information may be needed, for example, to ensure safety, to comply with the requirements of the government or of funding bodies, to provide support for staff or students or to implement institutional policies. In some of these cases, the University may need to seek specific consent from the individual.

6.3 Information Collected by the University website

Information collected on the Bangor University website is owned by Bangor University (including any subsidiary companies). The University will not sell, share or rent this information to others in ways which differ from what is stated on the University's website or in any prior agreement. Specific information relating to Bangor University's website can be found in the University's Privacy and Cookies Policy.

6.4 Data Security Breaches

Any data-related incident or breach or potential breach of the Act, or other equivalent legislation or of the requirements of this Policy should be reported to the Head of Governance and Compliance as soon as possible and, in any case, within 24 hours of discovery. Incidents will be dealt with in accordance with the University's Procedures for the Management of a Suspected Data Security Breach.

6.5 Sharing of data with third parties

The sharing of personal and / or special categories data will comply with those details set out in staff contracts and the Data Processing Declarations for staff and students.

Staff, students and others whose personal and / or special categories data may be held by the University, should note that the University has a duty under the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism, and that this duty may involve the passing of information to the police / security services in certain limited cases, overseen by the requirements of

the University's Prevent Policy, and the Information Sharing Agreement between statutory partners in the North Wales area.

6.6 Request for Information by Law Enforcement Agencies

There are exemptions within the Data Protection Act which allow the University, under strict guidelines, to release information to law enforcement agencies without the consent of the individual whose information is being released, and regardless of the purpose for which the information was originally collected.

The University should respond to all such requests for information in a consistent manner and it therefore operates a Single Point of Contact system for all law enforcement requests which is overseen by the Head of Governance and Compliance.

A detailed procedure outlining how the University deals with such requests is included as Appendix 1 to this Policy.

6.7 Request for Information from Statutory Agencies

The University will seek to respond to requests for information from Statutory Agencies (e.g. Local Authorities) in relation to

- A child, young person or vulnerable adult;
- Proceedings / investigations relating to a child, young person or vulnerable adult.

in a consistent manner.

In relation to such requests the University will follow the guidelines laid down in the *All Wales Child Protection Procedures* and also the provisions of Section 115 of the Crime and Disorder Act. Such requests will be considered by the Head of Governance and Compliance on the understanding that the Agency is able to confirm that there is an overriding public interest to justify the disclosure, and in particular the University, in making its decision, will seek to satisfy itself that one or more of the following considerations are relevant:

- The disclosure is necessary for the prevention or detection of crime, prevention of disorder, to protect public safety or protect the rights and freedoms of others;
- The disclosure is necessary for the protection of young or other vulnerable people
- The risks posed by the individual
- The vulnerability of those who may be at risk
- The impact of the disclosure on the offender
- Is the disclosure proportionate to the intended aim
- Are there equally effective but less intrusive alternative means of achieving the aim
- Where there is an overriding public interest in favour of disclosure the University will, as set out in Section 1.5.3 of the All Wales Child Protection Procedures require the specific detail of the request, and whether the consent of the individual has been sought and / or given.

6.8 Coursework / Examination Marks / Publication of Examination Marks

Students will be entitled to information about their marks or grades for both coursework and examinations. However, as outlined in Schedule 2, Section 25(3) of the Act, this may take longer than other information to provide where a result has not yet been ratified.

When a subject access request is made for examination marks, the University is obliged to respond by the earlier of:

- 40 days after the announcement of the results OR
- Five months from the receipt of the request, the fee and all reasonably required information.

Unless students are informed in advance and given the chance to opt out, the publication of exam results in an identifiable format either online or in a publicly accessible area of the University would not be acceptable under the requirements of the Act and this Policy. Students should be informed as early as possible in the academic year what the procedure will be for accessing their examination results.

7. Complaints

The Head of Governance and Compliance will coordinate any complaints received in respect of this policy.

- The complaint should be addressed to the Head of Governance and Compliance in the first instance. The complaint will be acknowledged immediately and every reasonable effort will be made to offer a more comprehensive reply within 21 days.

- If the applicant is not satisfied with the reply then they should inform the Head of Governance and Compliance within 21 days. The complaint will then be forwarded to the University Secretary and will be dealt with in accordance with the University's Staff & General Complaints Procedure or the University's Student Complaints Procedure as appropriate.

If applicants are dissatisfied with the outcome of the Complaints Procedure they may seek an independent review from the Information Commissioner. Requests for review by the Information Commissioner should be mad e in writing to:

The Information Commissioner, 2nd Floor Churchill House, Churchill Way, Cardiff CF10 2HH Tel: 02920 678 400

8. Contacts

Head of Governance and Compliance, Governance and Compliance Office, Bangor University, College Road Bangor Gwynedd LL57 2DG Tel: (01248) 38 2413 E-mail: info-compliance@bangor.ac.uk

9. Relevant Legislation, Codes of Practice and Industry Standards

- Data Protection Act 2018
- General Data Protection Regulation
- Counter Terrorism and Security Act 2015
- Freedom of Information Act 2000
- Limitation Act 1980

10. Related Policies and Procedures

Other relevant University policies include, but are not limited to:

- Records Management Policy
- Freedom of Information Policy
- Information Security Policy
- Procedures for the Management of a Suspected Data Security Breach

- Guidance on the Destruction of Records Containing Confidential Data
- Prevent Policy
- Higher Education Statistics Agency (HESA) Collection Notices for Students and Staff
- CCTV Code of Practice

Appendix 1

Disclosure Procedure: Request for Information by Law Enforcement Agencies

1. Background

These Procedures are intended to cover situations where the University receives requests from the Police or other organisations / agencies with law enforcement responsibilities (such as the Department for Work and Pensions, local authorities, HM Customs and Revenue and the UK Visas and Immigration) for personal information about students, staff or other individuals whose information the University holds. These Procedures also include requests for the provision of any CCTV footage2.

Personal information held by the University is managed in accordance with the Data Protection Act 2018 (the Act) and the University's Data Protection Policy3. The Act and the University's Policy provide guidance on the circumstances when it is lawful to disclose and transfer personal information outside the University and in general this should be carried out "fairly and lawfully" and in accordance with the University's Data Protection Notification.

There are, however, exemptions within the Act which allow the University, under strict guidelines, to release information to law enforcement agencies without the consent of the individual whose information is being released, and regardless of the purpose for which the information was originally collected.

In particular personal information may be released if:

- the information is required for safeguarding national security
- failure to provide the information would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty

Personal information may also be disclosed without contravening the terms of the Act where that disclosure is required by law.

Before the University releases any information to a law enforcement agency it must satisfy itself that the disclosure is necessary and required for a legitimate purpose.

The University seeks to co-operate with the police and with other agencies in the prevention and detection of crime and these Procedures set out the steps to be followed when responding to requests for personal information from these external agencies.

These Procedures should also be considered in conjunction with the University's Prevent Policy and its Information Sharing Agreement with partners to the Prevent and Channel Programme.

2. Requests for Information

It is important that the University responds to all requests for information in a consistent manner and the University therefore operates a Single Point of Contact system for all law enforcement requests which is overseen by the Head of Governance and Compliance, Governance and Compliance Office. To facilitate this any member of staff who receives a request for personal information from the Police or any other agency with law enforcement responsibilities must forward it as soon as possible to the Compliance and Records Officer or the Head of Governance and Compliance. The Head of Governance and Compliance will then ensure that the request is handled in accordance with the remainder of these Guidelines. Further advice on requests for information from the police or other agencies should be directed to the Head of Governance and Compliance.

Staff should not feel pressurised to disclose information "on the spot", as it is very rare that the police or agencies require the information urgently (although such circumstances are dealt with in Section 4 below).

3. Governance and Compliance Office Procedures

[a] Police Requests

All police forces have standard forms which must be used to request personal information from Bangor University, in accordance with guidance issued by the Association of Chief Police Officers. The form must certify that the information is required for an investigation concerning national security, the prevention or detection of crime or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information. All requests from the police, (apart from emergency requests, which are dealt with at section 4. below,) should be received on a data protection form, should clearly state all the information being requested and should be signed and dated by an officer of the rank of Sergeant or above.

[b] Other Agencies with Law Enforcement Responsibilities

Other agencies may not routinely use standard forms to submit their requests. However, any request for personal information should:

- Be in writing, on headed paper, and signed by an officer of the agency;
- Describe the nature of the information which is requested;
- Describe the nature of the investigation in broad terms, including citing any relevant statutory authority for requesting the information;
- Certify that the information is necessary for the investigation.

On receipt of such a request the data would normally be disclosed, after due consideration of the University's legal position to provide such data, by the Head of Governance and Compliance.

4. Requests for Disclosure of Information in Emergency Situations

The University acknowledges that, from time to time and in extraordinary circumstances, police forces, other law enforcement agencies or other emergency services may urgently require personal data from the University and may not be in a position to complete the usual required paperwork at that time. These requests are usually received by the University's Security Section but may be received by any member of staff. Requests of this type would include urgent requests for provision of CCTV footage for genuine police operational reasons and / or requests for contact information for members of staff or students.

In these circumstances, during normal office hours, staff should contact the Compliance and Records Officer or the Head of Governance and Compliance, in the first instance for advice and authorisation before providing any information / CCTV footage.

If the request is being dealt with out of normal office hours, during University holidays or at a weekend and information or images are required immediately to deal with an ongoing police or other law enforcement incident the procedures outlined below should be followed:

1. The University's Security Section should note all of the emergency information required, the circumstances of the request and the name, rank and number of the requesting Police Officer.

2. Authorisation and / or advice should then be sought advice from the Campus Services Manager (Security) or Deputy.

3. Where the request isn't straightforward, or the information isn't easily located the Campus Services Manager (Security) or Deputy may seek advice from the Head of Governance and Compliance.

4. Once the release of information or images is authorised the Security Team Leader or Assistant should note in the security log the exact circumstances of the request, the name, rank and number of the requesting Police Officer. This information should be forwarded to the Compliance and Records Officer and the Head of Governance and Compliance as soon as practicably possible.

5. If information / images are released in emergency circumstances the Governance and Compliance Team will ensure that the request is followed up with a formal written request from the relevant law enforcement agency, either by supplying a data protection form or a letter on headed paper appropriately authorised.