PRIFYSGOL BANGOR UNIVERSITY

INFORMATION SECURITY POLICY

Rev	Date	Purpose of Issue/ Description of Change	Equality Impact Assessment Completed
1.	June 2011	Initial Issue	
2.	29th March 2012	Second Version	
3.	15th April 2013	Third Version	
4.	8th June 2015	Fourth Revision	28th July, 2015
5.	28th January 2019	Fifth Revision	

Policy Officer	Senior Responsible Officer	Approved By	Date
Head of Governance and Compliance	Director Corporate Services	Compliance Task Group	28th January 2019

This Policy will be reviewed in 3 years

Information Security Policy

1. Introduction

1.1 It is Bangor University's policy that:

[a] the information that it manages (both manual and electronic) shall be appropriately managed and secured to:

(i) ensure compliance with relevant legislation and guidance; and,
(ii) ensure information is made available solely to those who have a legitimate need for access, and to protect against unauthorised access; and,
(iii) ensure confidentiality is maintained, especially where third party or personal data is held; and,
(iv) ensure business continuity and the protection of assets;
(v) prevent failures of integrity, or interruptions to the availability of that information.

[b] Staff are trained in information security policies and practices.

[c] Specialist advice on information security is made available throughout the University

[d] University systems, technology and applications used to store or process personal, sensitive or confidential data are secured, authenticated and backed-up.

[e] Any breaches or near breaches of information security are reported to ensure that appropriate actions, and preventative measures are taken

1.2 This Information Security Policy provides management direction and support for information security across the University. Specific subsidiary policies and guidance shall be considered as part of this Policy. Through these policies, procedures and structures, the University will facilitate the secure and uninterrupted flow of information, both within the University and in all external communications.

1.3 This Policy has been approved by the Compliance Task Group and ratified by the Executive and forms part of Bangor University's policies and procedures. It is applicable to and will be communicated to staff, students and other relevant third parties.

1.4 All breaches of this Policy, whether accidental or deliberate, actual or suspected shall be reported and investigated in accordance with Section 8 of this Policy.

2. Definition

2.1 For the purposes of this Policy information security is defined as the practice of ensuring information is only read, heard, changed, transmitted, broadcast and otherwise used by people who have a right and need to do so.

2.2 Information within the University exists in many forms. For example information could be:

- printed or written on paper,
- stored electronically,
- transmitted by post or using electronic means,
- broadcast,
- spoken

3. Responsibility for Information Security

3.1 Any infringement of this or any subsidiary policy or guidance will be treated seriously by the University and may lead to disciplinary action and / or legal proceedings.

3.2 Information security is the personal, professional and legal responsibility of all staff (including contractors, short term, voluntary staff and anyone with a University IT account) and students. Every person handling information or using University information systems is expected to have proper awareness of and observe the policies and procedures noted within this Policy, both during and, where appropriate, after their time at the University and to act in a responsible and professional way.

3.3 Deans of College, Heads of School and Directors of Professional Services shall be responsible for monitoring and maintaining awareness of this Policy within their College / School / Service.

3.4 This policy may be supplemented by more detailed interpretation for specific sites, systems and services.

3.5 Implementation of the Policy is managed by the Head of Governance and Compliance in consultation with those Senior Officers with specific information security responsibilities within the University.

3.6 Further guidance on information security can be found in Appendix 1.

4. Application of this Policy

4.1 This Policy shall apply to all locations from which University systems, data or information are stored or accessed, whether for research, human resources, student admissions or other activities. This shall extend to home use and all other off-University sites where applicable.

5. Compliance

The University is required to maintain security in compliance with legislation, including but not limited to the following:-

[a] Data Protection

Bangor University holds and processes personal information about staff, students and third parties for the purpose of academic, administrative and commercial reasons. Responsibilities under the 2018 Data Protection Act and the General Data Protection Regulation (GDPR) are set out in the University's Data Protection Policy.

[b] Counter-Terrorism and Security Act

The University has a statutory duty to prevent people from being drawn into terrorism (under the Counter-Terrorism and Security Act 2015). Staff and students should not carry out any acts which could incite or promote extremism including, but not limited to, accessing websites or sharing material that might be associated with extremist or terrorist organisations.

[c] Copyright

It is the University's policy to comply with all legal obligations and to ensure that no copyright material is either copied without the owner's consent or copied in any way which falls outside the remit of the University's collective licensing schemes.

[d] Records Management

Guidelines on the retention, storage, handling and disposal of the University's records and information are set out in the University's Records Management Policy.

Data retention periods for email (and all other records) are set out in the University's Retention Schedule. For Office365 records (including emails) are permanently deleted one month after deletion from a User's account.

All members of staff have a responsibility to ensure that personal information used within the course of their work are securely disposed of. Further guidelines can be found in the University's *Personal Information Disposal and Retention Guidelines.*

[e] IT Resources

[i] The University's IT Resources are provided on condition that they are used for acceptable, authorised purposes only. A statement of users' responsibilities with respect to IT resources is set out in the University's *Acceptable Use Regulations*. Users' responsibilities with regard to the disposal and re-use of IT equipment is set out in the University's *Policy for the Re-use and Disposal of Computers, other IT Equipment and Data Storage Media*.

[ii] The document *Policy on Use of Social Media and other Third Party Websites* also gives staff guidelines on appropriate use of systems.

[iiii] all mobile devices[1] purchased by the University or personal devices used by members of University staff to remotely access University data must be encrypted, and must be secured by userid for laptops and PIN protected for smartphones and tablets[2]. Unsecured devices should never be used to store University data.

[iv] Video cameras/voice recorders also store data and information that must be secured both physically and through encryption (where possible). Personal video or audio based data should never be left on an unencrypted device. See Appendix 1 for further guidance.

[1] Such as laptops, Smartphones, tablets and voice recorders

[2] Encryption is possible on approved university laptops (PC & MAC) and approved smartphone/tablet devices. IT services are able to advise and setup such devices in a secure encrypted manner.

[v] It is not possible, within Office 365, for members of staff to forward their entire email account off site to a third party email host. If members of staff choose to forward one off emails this should be done with due regard to the requirements of this Policy and the *Acceptable Use Regulations*.

[f] Caldicott Report 1997

The Caldicott Report sets out recommendations for maintaining security of patient's details and is of particular importance to certain University Schools who should ensure that they are fully aware of the requirements of the Report.

[g] University Business Systems

A Data Owner is defined for each University business system (e.g. the student records, human resources and / or finance systems). The Data Owner should ensure that an annual audit is carried out of all registered users of the system to ensure that users continue to have the most appropriate level of access.

Deans of College, Heads of School and Directors of Professional Services should ensure that any other databases within their sphere of responsibility have a designated data owner, relevant access control and that similarly an annual audit is carried out of all registered users of the database.

[h] Non University related information

Individuals are personally responsible for any non-work related information which they hold, in either manual or electronic format, on University systems and premises. The University takes no responsibility for this information.

6. Information Security Training & Risk Assessments

6.1 The University recognises the need for all staff, students and other users of University information to have access to information security training. This training will be facilitated by the Governance and Compliance Office and IT Services in consultation with other relevant University Professional Services.

6.2 The Dean of College, Heads of School and Directors of Professional Services (via an appropriate officer) shall be accountable for ensuring that regular risk assessments are undertaken so to understand what information they hold and what security arrangements are necessary in order to protect such information from any security breaches and whether such arrangements are actually put into effect.

6.3 Deans of College, Heads of School and Directors of Professional Services must provide an annual return to the Compliance Task Group for its first meeting of the academic year confirming that, within their area of responsibility, the requirements of this Policy are being complied with.

6.4 The Compliance Task Group shall be responsible for monitoring compliance with paragraphs 6.2 and 6.3 above, including undertaking regular audits and making recommendations as appropriate.

7. Business Continuity

The University manages its business continuity processes through the requirements of the Emergency Management Policy which includes the requirement for Deans of College, Heads of School and Directors of Professional Services to put in place a business continuity plan. A list of the University's corporate contingency plans can be obtained from the Head of Governance and Compliance, Governance and Compliance Office.

8. Incident Reporting and Complaints

8.1 All breaches of this Information Security Policy should be reported immediately to the Head of Governance and Compliance in the Governance and Compliance Office using the form in Appendix 2 with the exception of staff or students who inadvertently disclose their IT account password. In this instance the individual must change their password **and** notify the IT Services Helpdesk on 01248 388111 **immediately**[3], to ensure remedial action can be taken to limit the widespread impact of such disclosure.

8.2 It is important to report any breach as quickly as possible so as to minimise the potential damage to the University (including reputational), minimise distress to individuals and to reduce the risk of heavy fines under the requirements of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

8.3 Under no circumstances should any person attempt to conceal a breach. Concealment of such a breach could lead to disciplinary action and the Information Commissioner's Office may also take individual action.

8.4 The University also has a *Public Interest Disclosure (Whistleblowing) Policy*. This allows individuals who have concerns over another person's actions such as security issues or misuse of information to raise such concerns in a structured and constructive manner.

[3] If outside helpdesk hours, email helpdesk@bangor.ac.uk

APPENDIX 1

Information Security Guidelines

1. Keeping Personal Information Secure

All personal data must be stored in a secure environment with controlled access – the level of security applied to the information will depend on the nature of the information and should be applied following a risk assessment which should establish the potential risk of unauthorised access and / or theft.

[a] Paper records

Appropriate storage for paper / manual records would include:

- Locked metal cabinets with keys limited to authorised staff only;
- Locked drawer in a desk (or other storage area) with keys limited to authorised staff only;
- Locked room accessed by key or coded lock where access to the key/code is limited to authorised staff only;

[b] Electronic records and Database Systems

Good practice guidelines for electronic records would include:

- **Never disclose your password(s)** – you will never be asked to disclose your password, and never reply to any email requesting you disclose you password – if in doubt check with IT Services;
- Ensure your password is robust – not a real word or name, a mixture of letters, number, capitals, and lower case – change it regularly and refer to the ITS website[4] for guidance
- Always log off, or lock a workstation before leaving it;
- When confidential work is being carried out ensure no one else can read the screen;
- Protect equipment from physical theft, this is vitally important for portable equipment such as laptops and mobile phones;
- Store all records on the University network (One Drive, M or U drive) – this ensures data is backed up by IT Services, and mitigates the risk of information loss/disclosure due to sharing a computer or computer theft. Where it is not possible, ensure that all important data is backed up regularly and backups are kept in a separate secure location. Liaise with IT Services if you require assistance.
- Ensure your level of access to database systems containing personal information (e.g. student system, finance system, HR system) is relevant to your job role and responsibilities. If your job/responsibilities change, notify the data owners of each system to ensure your access is appropriate.
- Particular care is required when forwarding emails, in particular ones with attachments so that information is only sent to people with a real 'need to know'. Before forwarding attachments at all you should check that the information is not available to them by other secure means.

[4] http://www.bangor.ac.uk/itservices/knowledgebase/faq/gpasswd.php

[c] Using IT Resources securely away from the University

[i] When using a PC or a MAC and working away from the University, you should be aware that information could be stored on that device in two key ways:

- you decide to store a file on the device, or
- through a process such as reading an email attachment, information is inadvertently left on the device unbeknown to you.

[ii] The **secure method** of working away from the University with due regard for Information Security (e.g. on a University laptop or non-University laptop/computer) is to use the University's Office 365 and /or *Desktop Anywhere*[5] service. This method ensures all information stays on the University controlled IT infrastructure, as is not stored on the device used. Having logged in, use the "Bangor University Staff Desktop" menu icon to experience working as if you were using PC at the University.

You can also access your Bangor University email and One Drive account securely through the Office365 web interface as the information is not stored on the device used.

[iii] Encrypted USB sticks must not be used under any circumstances to hold any University data (this would include emails, documents, research data etc.) Any exceptions to this rule should be approved, in advance, by the Head of Governance and Compliance who will ensure that there are no other secure methods available and an appropriate risk assessment is undertaken.

[d] Cloud Computing[6]

The use of cloud computing is increasing and its use is of benefit to members of staff working collaboratively or off site.

The University's calendar and email system is already cloud based (Microsoft Office365) and compliant with United Kingdom Data Protection legislation. The use of other email and calendar systems may not be and members of staff should ensure that the requirements of the Data Protection Act 2018, and the General Data Protection Regulation (GDPR) are maintained for any personal data which may be held within a cloud computing environment.

[e] Mobile Devices

Any University or personal smartphone/tablet which is configured to use the University's Office365 will automatically have a PIN number enabled, encryption enabled, and have remote wipe enabled to ensure that University data can be removed from the device in the event of its loss etc.

Individual members of staff have responsibility for managing and protecting their mobile device (for example an iPhone/Smartphone) and the data contained on it.

There are simple steps you should take to protect your mobile device and the data that is on it.

---

[5] http://www.bangor.ac.uk/itservices/desktopanywhere/

[6] Adapted from the JISC Legal Information Guide *Cloud Computing and the Law for Senior Management and Policy Makers*

- Ensure your device is encrypted (including any memory cards that maybe inserted into the device). Seek guidance from IT Services if needed.

- Setup a security password or PIN number on your mobile device. When the device is not used for a period of time, it will lock and need the security code to be used again, adding protection if the device is mislaid or stolen.

- Make regular back-ups of any data that is on your device, such as documents, images, etc. If you synchronise your email, calendar and contacts with your University account, you do not need to back-up this data as it is stored centrally at the University and only a view of this data is on your device. However, if you have documents, images, or additional data aside from your University account, you should regularly copy these files to your PC, ideally a folder on your One Drive, to make sure you have backup copies should your device fail or be lost.

[f] Audio and Video Recording Devices.

Audio and video devices are regularly used by members of staff and / or students for recording interviews, etc. You should be aware that such recordings, when they include any personal identifying information, are deemed to be personal data under the requirements of the Data Protection Act 2018, and the General Data Protection Regulation (GDPR), and must therefore be secured appropriately.

- The electronic alternatives to a dedicated camera or voice recorder should be considered in the first instance. Most if not all tablet devices and smartphones have cameras and the ability to record audio. The quality of recording on these devices is now very high – most new devices being HD video. Modern Android and Apple devices are also encrypted and may offer a simple solution to requirements. It must be remembered - encrypted tablets and phones are still easily lost or stolen so any data should be backed up to a secure location as soon as practically possible and removed from the phone or tablet to protect from loss.

- Please be aware that portable audio and video devices used for such recordings may be desirable targets for thieves. When not in use they must be stored locked in a secure locations out of sight. They should never be left visible in a vehicle, on public transport or left unattended in public areas.

- The University recommends that all audio and video devices used to store personal and / or sensitive personal data and / or confidential information are encrypted. It is possible to purchase audio recorders that use on-board storage memory and can be encrypted. Please contact the IT Helpdesk for advice on current devices.

- You should be aware that many commonly used audio devices and all portable video cameras use removable solid state memory devices (e.g. a micro SD card) which cannot be encrypted. Please ensure that these devices, whether being used by you or by students under your supervision / direction, are protected from theft and from unauthorised or accidental disclosure of personal, sensitive and / or confidential information.

- If you do not have access to an encrypted device for your recordings and you have identified that the records will contain personal, sensitive or confidential information then please consider whether it is necessary to record the information at all. Is there an alternative, possibly lower risk, manner of keeping or safeguarding the information?

- If, after considering all the options, you are forced to use an unencrypted device then you will need to take steps to immediately encrypt the data captured. On completion of the recording session the content should be transferred from the memory card used on to an encrypted device (usually a laptop). The files should then be erased from the memory card. As with USB memory sticks, when a file is deleted in the usual way it is not completely erased until it is overwritten and the user of the device will never know when that actually happens. Hence, data must be deleted with a free secure deletion utility such as Disk (http://www.diskwipe.org/). You must ensure that your data is successfully transferred to the secured device before doing this as it is a permanent action!

2. Access to Personal Data

a) Deans of College, Heads of School, and Directors of Professional Services should ensure they are aware of those staff members within their sphere of responsibilities who, by the nature of their post, have been identified as requiring legitimate access to personal data in the course of their employment.

b) The designated purposes for which access to the personal data will be permitted must also be defined. For some Colleges and Departments this will be clear by the nature of their function e.g. Human Resources. However in other cases these purposes will need to be specifically outlined.

c) As noted in the University's Data Protection Policy staff members 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 infringement of the Data Protection Act 2018 will be treated seriously by the University and may be considered under disciplinary proceedings

d) Where a file containing personal data is removed from the secure filing for a legitimate reason by an authorised member of staff a strict signing out and signing in procedure should be in force.

e) Staff should ensure that personal information is only photocopied where this is strictly necessary and should ensure that the copy and the original are subject to the same security protocols.

f) Unless absolutely essential, and authorised in advance by the relevant Dean of College, Head of School or Director of Professional Service , staff should not take personal data outside the University – in either manual or electronic form. Where it is essential for this to happen appropriate security precautions must be taken to guard against theft or unauthorised access to those data (see Section 1 above).

g) Where secure off-site access to electronic information and databases is required, the University's One Drive or *Desktop Anywhere* service should be used. This ensures that information is not physically transferred outside the University and the exchange of

information is over an encrypted link. To use the service a Bangor username and password is required.

h) Off-site access to email should be configured in accordance with ITS advice[7] to ensure secure transmission

3. Transfer of Personal Data / Sensitive Personal Data

a) Before transferring or disclosing personal data outside the University staff must familiarise themselves with the requirements of the University's Data Protection Policy. Particular care should be taken when forwarding any attachments via email (see point 1 [b] above).

b) Staff must ensure that appropriate security precautions are in place (such as encryption) to minimise the risk of losing the data and / or accidental disclosure of the data.

c) All postal communications containing personal data must be marked *strictly private and confidential* and must be addressed to a named individual.

d) Use of physical devices such as USB memory sticks, CDs or DVDs must not be used to send personal data unless previously authorised by the Head of Governance and Compliance.

e) For both external and internal mail containing personal data the most appropriate and secure method of sending the information must be considered. For external mail use of the Royal Mail "Signed For" service or a courier offering a tracking and signing service should always be considered. Further advice should be sought from the University Post room.

f) Sensitive personal data must not be emailed externally under any circumstances unless encrypted (contact IT Services for further guidance on availability of email encryption).

g) Manual personal data must always be sent by Royal Mail "Signed For" service or a Courier service offering a tracking and signing service.

h) Where possible wireless network connections should make use of secured services. In the University the preferred secure service is called *eduroam* (which will also work in many other Universities in the UK and abroad). The IT Services web site has information on connecting to the service. Assistance is also available via the IT Support Centre (X8111).

At home your wireless broadband connection should be set to a secure connection method called WPA2. Your internet service provider (ISP) can provide assistance.

In other public areas a secured service may not be available. In this case you should be aware that any data sent or received via normal web pages could be intercepted. Sensitive data on a unsecured network should only be sent using secured web pages (the address of these begins https:// - the 's' indicating secure).

i) Many web forms will ask you if you wish to save a password you have provided. In all cases choose the option – "never for this web site". This will help prevent any unauthorised access to any secured web pages.

[7] http://www.bangor.ac.uk/itservices/help/workfromhome/index.php.en

j) Avoid using the same password for both business and private use, and change your password regularly.

4. Further Information

Further information or guidance on any aspect of these Guidelines can be obtained from the Governance and Compliance Office or IT Services.

APPENDIX 2

INFORMATION SECURITY INCIDENT REPORTING FORM

Your Details

1. NAME ……..
2. DEPARTMENT ……..
3. EMAIL ……..
4. TELEPHONE ……..

Incident Details

1. Date of incident……
2. Date incident reported ……
3. Please provide a short summary of the security breach or loss of data. (please state type of information, such as commercial or personal data, medical records, financial, student or staff details):-

   ……
   ……
   ……
   ……
   ……
   ……

4. Please advise what follow up or other action has been taken (if any).
   ……
   ……
   ……

5. Any other information you feel is relevant

……
……
……

Please email to: Lynette Hunter, Governance and Compliance Office: info-compliance@bangor.ac.uk