INFORMATION SECURITY POLICY

Rev	Date	Purpose of Issue/ Description of Change	Equality Impact Assessment Completed

Information Security Policy

1. Introduction

1.1

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. Awareness raising in relation to the requirements of the policy also occurs via the Staff Bulletin and at the Deans & Heads meeting.

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 Services 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 access

[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 me/atimited

[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 is to use a University (encrypted) laptop. When accessing data off campus the VPN must be used. Contact the IT Helpdesk if you require VPN software on your university laptop.

Staff who work in a hybrid or remote way should request that their computer provided by Digital Services is a laptop. These are encrypted and pre-configured to use Bangor's Office365 services.

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] External storage devices eg, DVDS, "memory sticks" etc 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. If such permission is granted then content should be encrypted.

[d] Cloud Computing[4]

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

The University has subscribed to a number of cloud based services including Office365, Blackboard – these are compliant with United Kingdom Data Protection legislation. Cloud services not commissioned by the University must not be used. Any exceptions to this rule should be approved, in advance, by the Director of Digital Services.

[e]

- Ensure your device is encrypted (including any memory cards that maybe inserted into the device). Seek guidance from Digital 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, files, 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 Digital Services' 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

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.

g) Where secure off-site access to electronic information and databases is required, the University's One Drive, Teams or 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[5] 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). Staff must ensure that the recipient email is correct prior to sending the information.

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 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 Services.

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 Digital 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 (which will also work in many other Universities in the UK and abroad). The Digital 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 the University's VPN service.

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

i) Many web forms will ask you if you wish to save a password you have provided. In all cases choose the option –

APPENDIX 2

INFORMATION SECURITY INCIDENT REPORTING FORM
Please send to info-compliance@bangor.ac.uk

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

……
……
……

info-compliance@bangor.ac.uk