PRIFYSGOL
BANGOR
UNIVERSITY

Acceptable Use Regulations:
Regulations for the Use of IT Resources

Rev	Date	Purpose of Issue/Description of Change	Equality Impact Assessment Completed
1.	May 2009	Initial Issue	
2.	08/06/15	Update and approval by Compliance Task Group	28th July, 2015

Policy Officer	Senior Responsible Officer	Approved By	Date
Head of Compliance	University Secretary	Compliance Task Group	8th June 2015

These Regulations will be reviewed in 3 years

Acceptable Use Regulations:
Regulations for the Use of IT Resources

These regulations use a number of terms that are defined in section 3 below.

1. Overview

1.1 These Acceptable Use Regulations (AUR) are a statement of Users' responsibilities with respect to IT Resources. Authorised System Administrators are granted additional powers and are subject to additional regulations.

1.2 The University's IT Resources are provided on condition that they are used for acceptable, authorised purposes only. The main purpose of these AUR is to encourage responsible use of IT Resources; to maximise the availability of IT Resources for legitimate purposes; and to minimise exposure to misuse from inside or outside the University.

1.3 Use of the University's IT Resources implies, and is conditional upon, acceptance of these AUR, for which a signature or acknowledgement of acceptance may be required on joining the University, and periodically thereafter. The lack of a signature or acknowledgement however does not exempt an individual from any obligation under these regulations.

1.4 Failure to comply with these regulations could result in action under the University's Disciplinary Procedures, withdrawal of privileges or withdrawal of access to IT Resources. Where a User is suspected of breaching these AUR a User's account may be temporarily suspended until the conclusion of the university's Disciplinary Procedures. Under certain circumstances, breaches of these AUR may result in criminal or civil sanctions. Where the University is of the opinion that the usage may constitute a criminal offence, the University shall refer the matter to the appropriate law enforcement agencies, and any other organisations whose regulations may have been breached. The University accepts no liability where such steps are taken.

1.5 Bangor University reserves the right to recover from the User any costs (including legal costs) incurred as a result of their infringement.

2. Scope

These regulations apply to:

- The use of IT Resources provided by, or for which access is facilitated by, Bangor University;
- Any IT Resources owned by Bangor University, or IT Resources for which access has been facilitated by Bangor University;
- The use of IT Resources owned by other bodies, access to which has been provided by Bangor University. In such cases, the regulations of both bodies apply. In the event of a conflict of the regulations, the more restrictive takes precedence.

These AUR apply subject to and in addition to the law. Any infringement of these regulations may also be subject to penalties under civil or criminal law and such law may be invoked by Bangor University. Use of Bangor University's IT Resources may be logged to permit the detection and investigation of infringement of Policies and UK law.

3. Definitions

These AUR use a number of terms that are defined below:

User/Users
Any person or persons making use of the University's IT Resources. This includes but is not limited to:

- all Bangor University staff and students; and other authorised individuals, requiring IT Resources for furtherance of the University mission
- Individuals accessing the institution's online services from off campus;
- External partners, contractors and agents based on site and using Bangor University's network, or offsite and accessing the institution's systems;
- Tenants of the institution using the University's computers, servers or network;
- Visitors using the institution's WiFi;
- Students and staff from other institutions logging on using eduroam.

Authorised Systems Administrator
A member of staff who administers systems transmitting or holding information/data belonging to others. They are bound by legislation and are required to sign a declaration that they have read and understood the Charter for System and Network Administrators[1]

Designated Authority
The Designated Authority for IT Resources is whoever is responsible for their provision. Thus, in the case of centrally provided IT Resources, the Designated Authority will be the Director of IT Services, Deputy Director or nominee and, in the case of departmentally provided IT Resources, it will be the Dean of the College, School or Department concerned or their nominee.

Hacking
An abuse of the University's IT Resources. Such abuses include but are not limited to:

- Attempts to access or actions intended to facilitate access to computers, data, network equipment or information transmitted over the University network for which the individual is not authorised.
- Unauthorised resale of data or services.
- Attempts to damage or deny service from computer or network systems.
- Attempts to monitor data on the network or to introduce spoofed packets, forge routing or switching information.
- Deliberately scanning for or attempting to make use of any security bug or weakness.
- Deliberately introducing any virus, worm, trojan horse, spyware or other such software into any IT Resources, or taking action to circumvent any precautions taken or prescribed by the University to prevent this.

[1] https://community.jisc.ac.uk/library/janet-services-documentation/suggested-charter-system-administrators

Information Technology Resources (IT Resources) For
these AUR IT Resources are defined as:

- IT equipment (e.g. computers, printers, university network wired and wireless, multi-function devices e.g. Xerox copier/printers)
- Any information technology facilities or services provided by the university (e.g. computer rooms for student use, the network in halls of residence)
- Software (e.g. Office365, Microsoft Word)
- Communication/storage of information and any operation involving the manipulation, transmission or viewing of data by electronic means, within Bangor University, within the UK or internationally.
- Any information captured through use of the university's IT Resources, including but not limited to systems logs, CCTV recordings and card access logs
- The University telephone system, which runs over the University network
- Online Cloud based services such as Office365 or any other online resources
- Accessing Bangor IT resources off campus via wireless, use of eduroam at other institutions etc.

4. Acceptable Use

4.1 University IT Resources, including an IT account, are provided for students to support their university education, for staff as part of their employment, and for other authorised individuals in furtherance of the University mission.

The University shall not prevent Users from using the IT Resources for personal non-commercial use, subject to adhering to the principles of these AUR. However, these AUR do not provide the Users with a formal right of access and such privileges may be revoked at any time. Where a potential User does not require access to IT Resources for the purposes of their employment or studies there shall be no obligation on the University to provide any IT Resources.

4.2 University IT Resources shall be used in an approved, ethical and lawful manner to avoid loss or damage to University operations, image, or financial interests.

4.3 Where the University's IT Resources are being used to access other resources, any action deemed abuse by the regulations of that resource, or illegal under UK law, this will be regarded as abuse under these AUR. These AUR are taken to include the Joint Academic Network (JANET) Acceptable Use Policy (AUP)[2] and the terms of the various software and data licence schemes under which the University has agreed access, e.g. Microsoft Campus.

4.4 Use of IT facilities for non-institutional commercial purposes[3] or for personal gain is not permitted.

5. Conditions of Use

Access to the University's IT Resources is subject to the following conditions:

5.1 Users undertake to comply with the provisions of all of the relevant Acts of Parliament, other relevant legislation and legal precedent. A list of relevant legislation is included in Appendix 1. The University reserves the right to take legal action against any User who causes it to be involved in legal proceedings as a result of use of the University's IT Resources. Users shall indemnify the University for any loss or

[2] http://www.ja.net/company/policies/aup.html

[3] The University's *Policy on Consultancy* should also be consulted.

damage, whether direct or indirect, suffered or incurred as a consequence of actions prohibited by these AUR.

5.2 IT Resources are provided entirely at the risk of Users. The University will not be liable for loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), damage (including damage to hardware, software or data) or inconvenience arising directly or indirectly from the use of the IT Resources.

5.3 Use of the University's IT Resources is provided for registered students and staff with a contract of employment. Any other persons having a legitimate role in the business of the university (e.g. visiting lecturers) may request a computer account via their College/School or Department.

5.4 Users handling, accessing or storing personal, confidential or sensitive information, must take all reasonable steps to safeguard it and must observe the University's Data Protection and Information Security policies and guidance. Where University or user owned mobile devices (e.g. laptops, tablets, smartphones, voice recorders) or removable media (e.g. memory sticks, external hard drives etc.) are used to store or access personal, sensitive or confidential data, they must be encrypted.

5.5 All Users of University IT Resources must ensure that any personal computer or device, for which they have responsibility and which is attached to the University network (wireless or wired), is adequately protected against viruses, malware and other malicious software through the use of up to date antivirus software and ensuring that operating system patches are applied regularly. All University computers provided for student use have up to date anti-virus software installed, and operating system patch updates enabled.

5.6 All individually allocated cards, usernames and passwords and other IT credentials are for the exclusive use of the individual to whom they are allocated. Passwords should not be divulged, even to Authorised System Administrators or Designated Authorities. Users are personally responsible and accountable for any use made of their accounts, logon IDs, passwords, passphrases, cards, PINs and tokens. Users must not use an obvious password, or record them where there is any likelihood of anyone finding them. Passwords must be changed at regular interval. **Users who inadvertently disclose their IT account password must change their password immediately and notify the IT Services Helpdesk on 01248 388111 immediately[4], to ensure remedial action can be taken to limit the widespread impact of such disclosure**.

5.7 Users accessing personal, sensitive or confidential information from off campus, must use an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service. You must also be careful to avoid working in public locations where your screen can be seen. Advice on working remotely with protected information is available in the University's *Information Security Policy.*

5.8 Users must adhere to the terms and conditions of all licence agreements relating to IT Resources; these include software, data, equipment, services documentation and other goods. Observance of these Acceptable Use Regulations will normally meet such requirements. Where software is purchased by a user/department for use on University owned IT equipment, the specific provisions of the license must be complied with.

5.9 In the use of IT Resources, Users shall have regard to the University's Intellectual Property Policy and the intellectual property rights of third parties, especially when downloading, forwarding and using

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

materials which are protected by copyright and/or contain branded materials. For example logos, pictures, text, video files, charts and/or icons.

5.10 Users shall supply the key to any encrypted data they own held on University computer equipment or passed through University networks if requested to do so by the University.

5.11 When University owned IT equipment (e.g. computers/printers) is no longer required, it must be reused or disposed of according to the IT Equipment Re-use and Disposal Policy. University software licenses and information/data must be removed, especially that which is considered personal or sensitive under the Data Protection Act 1998. The policy ensures that IT Equipment is disposed of in line with current legislation and other University policies (e.g. the Waste Electrical and Electronic Equipment (WEEE) directive, the Data Protection Act and the University's Records Retention Schedule).

5.12 The University's email disclaimer shall appear on all emails sent from University email accounts. The disclaimer will appear as standard on emails sent from all Users accounts, and must not be altered or removed.

5.13 University staff must adhere to Bangor University's Social Media Policy.

5.14 Users must ensure that they do not risk physically damaging the University's infrastructure.

5.15 Users should be aware that if they are using services that are hosted in a different part of the world, they may also be subject to foreign jurisdiction / laws.

5.16 Users shall ensure that the sending of personal data via email or over the internet is strictly necessary and in compliance with Data Protection legislation, including but not limited to the Data Protection Act 1998. In considering whether to store or send confidential or sensitive information using the University's IT Resources, Users should note the monitoring provisions of these AUR and also that all electronically stored information, including emails can be the subject of a request for information under the Freedom of Information Act. Any matters which are confidential or sensitive, should be clearly marked as confidential (e.g. in the subject box of an email), but it should be noted that this does not exempt the information from a Data Protection request or a Freedom of Information request. Further guidance can be found in the University's Information Security Policy.

5.17 Where use of IT Resources would contravene these AUR, but use is required for legitimate university study or business (such as lawful research), Users should request a partial exemption of the relevant sections of these AUR from the relevant Dean of College or Head of School and then obtain formal authorisation from the Head of Compliance, Planning & Governance Office.

5.18 Users should be aware that the University has a statutory duty to prevent people from being drawn into terrorism (under the Counter-Terrorism and Security Act 2015). Users 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.

6 Prohibitions

Users are prohibited from the following:

6.1 Using IT Resources in any way that is fraudulent, offensive, obscene, racist, malicious, defamatory, libellous, abusive, pornographic, sexual, indecent, constitutes a criminal offence (directly or indirectly), which

promotes extremism / terrorism and / or could constitute grooming children or other crimes against minors.

6.2 Using IT Resources in a way which is designed or is likely to cause harassment, bullying, inconvenience or upset to another or breaches confidentiality.

6.3 Sending/posting unsolicited advertising, spam, sending e-mails/postings that purport to come from an individual other than the person actually sending the message (e.g. using a forged address), chain letters, pyramid schemes or other "nuisance" messages.

6.4 Breaching a third party's intellectual property rights, including but not limited to licences, copyright, trademarks or music piracy

6.5 Corrupting or destroying either University or a third party's data or information. It is against the law to destroy information required either for a Freedom of Information Act or a Data Protection Act request.

6.6 Any activities that may be described as "hacking". Hacking is defined here as the intent to cause, or actions committed knowing they are likely to cause, wrongful loss or damage or alteration to information residing on a computing resource or any action that attempts to gain unauthorised access to, or diminishes the value of, or reduces the utility of, or affects injuriously by any means an IT Resource. Hacking is further defined in the Definition of Terms.

6.7 Deliberately wasting staff time or IT Resources (e.g. network bandwidth, processing power). Users shall take reasonable care not to disrupt the work of others and are prohibited from using the University's IT Resources in a way that denies service to other Users or affects the image or reputation of the University

6.8 Loading or reconfiguring any software or data on University computers provided for student use without permission from IT Services or for computers provided by Colleges, Schools or Departments, the Designated Authority within that College, School or Department. Where software is identified that would assist your University studies, you may suggest loading that additional software by contacting the IT Services Support Centre (helpdesk@bangor.ac.uk) where a decision will be made based on that software's general applicability and affordability.

6.9 Connecting or attempting to connect any device which extends the University's network or computing services (e.g. connecting wireless access point(s), router(s), mini-switch(es), broadband line(s) etc.) without the express approval of IT Services. Connection to the University's network with personal devices (e.g. computer, phones etc.) is prohibited in PC rooms provided for student use, but is permitted on the rest of the university network (wired, wireless, ResNet etc) subject to the other provisions of these regulations (e.g. the provisions in section 5.5).

6.10 Using IT Resources for any private commercial use, including, but not limited to private/personal consultancy work except that approved under the University's Consultancy Policy.

6.11 Using IT Resources to enter into a legally binding contract unless expressly authorised to do so by the relevant Dean of College, School or Central Department.

6.12 Disposing of University IT equipment other than in line with the IT Equipment Re-use and Disposal Policy.

6.13 Users must not attempt to monitor the use of the IT Resources. This would include:

- Monitoring of network traffic;
- Network and/or device discovery;
- WiFi traffic capture;
- Installation of key-logging or screen-grabbing software that may affect other users; ● Attempting to access system logs or servers or network equipment.

7. Monitoring and Privacy

7.1 UK legislation and University regulations require the University to inform Users how it will protect the privacy of their communications and data. Users should be aware that some system administrators have access to system information, including, but not limited to:

- event and usage logs, network traffic,
- data stored by Users using University IT resources (including files, emails, data in databases etc.), CCTV image recordings of the university estate,
- information stored by the university card access system (for entry to rooms e.g. student PC rooms) etc.

7.2 The University reserves the right to monitor and/or record communications and data as it deems appropriate:

- To establish the existence of facts to ascertain compliance with UK law or University regulations or procedures,
- In the interests of national security,
- To comply with lawful requests for information from government and law enforcement agencies, To prevent or detect a crime,
- To investigate or detect unauthorised use of systems, and, where necessary following the authorisation of a member of the University Executive , report such unauthorised use to the police, To secure, or as an inherent part of, effective system operation.

Such monitoring shall be in accordance with relevant legislation as listed in Appendix 1.

7.3 The University reserves the right to require the removal or amendment of personal information from its IT Resources.

7.4 Where a User is unable to fulfil their duties at the University (e.g. on sick leave, long-term absence, maternity leave, holiday or if a user has left the University), the University reserves the right to access the User's IT account (including email, data files etc.) in order to ensure continuity of the University's day-to-day business to ensure its business needs are met. (See Section 8 below).

7.5 Cyber Security - network traffic and data stored may be monitored for threats such as viruses, spam, phishing attacks, hostile and inappropriate activity etc. and may be modified to remove such threats.

7.6 System Administrators may use information gained from monitoring (e.g. from event and usage logs) to ensure the normal operation of IT systems and services but may not exploit or release any personal, sensitive or confidential material to the University or to a third party without the authorisation of the Head of Compliance and the receipt of appropriate paperwork. System Administrators should consult the Director/Deputy Directors of IT Services if in doubt. The Head of Compliance will ensure that

relevant legislation (e.g. Data Protection Act) and procedures for release of personal, sensitive or confidential information are followed. Examples of such releases would be:

- To comply with lawful requests for information from government and law enforcement agencies
- In cases where there are grounds to believe that there has been a breach of University regulations,
- Where access to University data is essential for operational reasons

7.7 System administrators may copy User data or lock an account to preserve evidence until such time as approval for further investigation can be granted.

8. Business Continuity Arrangements and Exit Procedures for Users' IT Accounts and Resources

8.1 The information contained in Users accounts (including data, documents, emails etc.) may be required in their absence in order to ensure continuity of the University's day-to-day business and to ensure its business needs are met.

8.2 Under normal circumstances Users who are expecting to be away from their duties/studies on a temporary basis, or those leaving their studies, leaving employment, or relinquishing their IT account should make arrangements in advance with their School/Department to ensure business continuity.

8.3 Users should not divulge their password(s) to anyone, but should ensure relevant information from their University IT account is shared with other authorised users, for example, by storing required documents on the U drive with appropriately secured access, by giving access to other members of staff to their Blackboard resources, by forwarding relevant emails and / or by putting an email auto-reply on their email account to inform enquirers whom they should contact.

8.4 When a member of staff leaves the employment of the University, or a student is no longer registered as a current student, or any other User leaves, the right to use the University's IT Resources (including the use of the bangor.ac.uk email address) shall cease immediately, unless otherwise expressly agreed in writing by the Dean of College/School/Department. This permitted extension of the use of the IT Resources shall be for a set period of time after which the rights under this extension shall automatically cease. Normally user accounts will expire a short period after the leaving date recorded in the student records or human resources system.

8.5 In exceptional circumstances where the University cannot ensure business continuity through the arrangements made above (e.g. an unexpected absence, the death of a User, where an account needs to be kept beyond its initial expiry date or the arrangements made prior to departure are not sufficient), the University reserves the right to access a User's IT account. Such access will be managed in accordance with the University's *Policy on Institutional Access to Staff and Student IT Accounts and IT Equipment* (included as Appendix 2).

8.6 All Users shall also ensure that before they leave the University that they return all University IT equipment to their College/School/Department in reasonable but working condition. The receipt of such equipment shall be confirmed in writing.

9. Disclaimer

Bangor University makes no representations about the suitability of its IT Resources for any purpose. All warranties, terms and conditions with regard to this service, including all warranties, terms and conditions,

implied by statute or otherwise, of satisfactory quality, fitness for a particular purpose, and non-infringement are excluded to the fullest extent permitted by law.

Bangor University shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with the use of the service, or with any delayed access to, or inability to use the service and whether arising in tort, contract, negligence, under statute or otherwise. Nothing in these terms excludes or limits liability for death or personal injury caused by the negligence of Bangor University in providing this service.

10. Incident Reporting and Complaints

10.1 All breaches or suspected breaches of the Acceptable Use Regulations should be reported immediately to Head of Compliance, Planning & Governance Office

10.2 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 which could potentially be significant (£500,000) for breaches of the Data Protection Act 1998.

10.3 Under no circumstances should any person attempt to conceal a breach. Such a breach could lead to disciplinary action and the Information Commissioner's Office may also take corporate or individual action.

10.4 The University also has a Whistle Blowing 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.

11. General

11.1 The invalidity or unenforceability of any provision of this AUR shall not prejudice or affect the validity or enforceability of any other provision of this AUR.

11.2 Other than by the University and the User, the parties to this AUR do not intend that any of its terms will be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 by any person not a party to it.

11.3 This AUR shall be construed in accordance with English and Welsh Law and the parties agree to submit to the exclusive jurisdiction of the English and Welsh Courts.

Appendix 1

Legislation relevant to the use of IT Resources includes, but is not limited to:-

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984

- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Counter-Terrorism and Security Act 2015
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and 2013

For example, this means that Users cannot:

- Create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- Create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety;
- Create or transmit material with the intent to defraud;
- Create or transmit defamatory material;
- Create or transmit material such that this infringes the copyright of another person or organisation;
- Create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe;
- Deliberately (and without authorisation) access networked facilities or services.

Appendix 2

Policy on Institutional Access to Staff and Student IT Accounts and IT Equipment

This Policy should be read in conjunction with Bangor University's Acceptable Use Regulations and with any relevant sections of Bangor University's Rules and Regulations as applicable to students and relevant terms of Bangor University's Terms and Conditions of employment as applicable to members of staff.

1. Purpose

1.1 The purpose of this Policy is to outline the circumstances in which it is permissible for Bangor University to access the IT accounts, communications and/or other data stored on IT equipment including any peripheral devices or hardware of staff members or students.

1.2 This Policy applies to all Bangor University ("University") staff, students and any other authorised users of the University's IT equipment and facilities.

1.3 The University respects the privacy and academic freedom of staff and students. However, the University may carry out lawful monitoring of IT systems. Staff, students and any other authorised users should be aware that Bangor University may access email, telephone and any other electronic communications, whether stored or in transit. This is in order to comply with the law and applicable regulations, to ensure appropriate use of the University's IT systems and for authorised business continuity purposes. All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000 (RIPA), the Human Rights Act 1998 (HRA) and the Data Protection Act 1998 (DPA).

2. Bangor University's Powers to Access Communications

2.1 Authorised University staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or maintained (except where the University acts solely as a service provider for another body) by the University, and may examine the content and relevant traffic data.

2.2 The University may access files and communications for the following reasons:

2.2.1 to ensure the operational effectiveness of the service. For example, the University may take measures to protect the telecommunications system from viruses and other threats such as hacking or denial of service attacks;

2.2.2 to comply with lawful requests for information from government and law enforcement agencies

2.2.3 in cases where there are grounds to believe that there has been a breach of University regulations,

2.2.4 Where access to University data is essential for operational reasons to establish the existence of facts relevant to the business of the institution, to ensure that all relevant

business information is retained and is available for the University's future business needs.

3. The Powers of Law Enforcement Authorities to Access Communications

A number of non-institutional bodies/persons may be allowed access to user communications in certain circumstances. Where the University is compelled to provide access to communications by virtue of a Court Order, warrant or other competent authority, the University will provide reasonable assistance and will disclose information to these non-institutional bodies/persons when required to do so and as allowed under the Data Protection Act 1998.

4. Policy on Access to Student Accounts by other Students

Students must not access the IT accounts of any other person, and must only use the institution's facilities in compliance with the University's Acceptable Use Regulations.

5. Policy on Access to Staff and Student Accounts by Authorised Persons

5.1 Staff Absence, Resignation, Retirement or Death in Service

For members of the Executive or senior members of staff please see Section 5.2 below

In cases where a member of staff is away from the University (for example on sick leave, long term absence, compassionate or maternity leave) or where the member of staff has resigned, retired or died whilst in service, the University reserves the right to access the member of staff's IT account (including email, data, files etc.) in order to ensure continuity of the University's day-to-day business and to ensure its business needs are met.

In such circumstances the University will follow the procedure set out below:

5.1.1 If appropriate, the member of staff will be contacted and consent sought for access to specific communications and/or documents.

5.1.2 Where consent is not given or cannot be given and there is no alternative way to obtain the required information, permission to access the member of staff's account will be sought in the first instance in writing from the appropriate Head of School or Director of Central Service who will in turn contact the Head of Compliance for authorisation.

5.1.3 Other than in exceptional circumstances, authorisation will normally only be given for access to specific information and not for general access to the account in question. Should general access to the account be required the exact reason for requesting this level of access should be given in writing to the Head of Compliance.

5.1.4 Following receipt of written authorisation from the Head of School / Director of Central Service Department the Head of Compliance will contact the IT Helpdesk to facilitate access.

5.1.5 The person authorised to access the account is responsible for ensuring that (unless prior authorisation is given to access the whole account) only the specific authorised information is accessed and that other information is not read or disclosed.

5.1.6 After the necessary information has been retrieved, the password to the absent member of staff's IT account will be reset and the new password will be communicated only to the absent member of staff.

5.2 Executive / Senior Member of Staff Resignation, Retirement or Death in Service

In cases where an Executive or senior member of staff resigns, retires or dies in service it is essential that the University ensures that information, emails and documents are preserved and that appropriate confidentiality and records management procedures are followed in order to ensure that all relevant business information is retained and is available for the University's future business needs.

In such circumstances the University will follow the procedure set out below:

5.2.1 If appropriate, prior to their departure from the University, the Executive / senior member of staff will be asked to ensure that only University business information remains within their account on their departure, and that all relevant information, data and emails have been shared with appropriate members of staff. The member of staff will also be informed that the University may seek access to their account for business continuity purposes once they have left the University.

5.2.2 Where consent is not given, or cannot be given, and there is no alternative way to obtain the required information, permission to access the member of staff's account will be sought, in the first instance, in writing from the Director of Human Resources (or the Vice-Chancellor in the case of the Director themselves) who will in turn contact the Head of Compliance.

5.2.3 Following receipt of written authorisation from the Director of Human Resources (or Vice-Chancellor) the Head of Compliance will:

- inform the Deputy Director of Human Resources (Operations);
- arrange for an out of office response to be placed on the account either immediately (if the member of staff is deceased or has already left) or the day following the last day of service;
- change the password on the account either immediately (if the member of staff is deceased or has already left) or the day following the last day of service. This password to be retained securely by the Head of Compliance;
- arrange to access the account along with the Deputy Director of Human Resources (Operations) and deal with any immediate matters;
- undertake a review of information including cataloguing emails and documents;
- arrange a forward on the email address linked to the account to an appropriate member of staff;

5.2.4 The final record of information should be placed into the care of the most appropriate Executive member of staff. This would normally be either the Director of Planning & Governance or the Director of Human Resources.

5.2.5 In the case of a death in service the requirements of the *Procedures for Dealing with the Death of a Member of Staff* should also be complied with.

5.3 Access to Student Accounts – Absence from University / Death whilst at University

In cases where a student is away from the University (for example on sick leave, long term absence, compassionate or maternity leave) the University reserves the right to access the student's IT account (including email, data, files etc.). It is envisaged that the need to access a student's account using this Policy will be extremely rare, and would only be necessary in order to ensure continuity of the University's day-to-day business and to ensure its business needs are met (for example where a student is working on a research project where access to data is required).

In such circumstances the University will follow the procedure set out below:

5.3.1 If appropriate, the student will be contacted and consent sought for access to specific communications and/or documents.

5.3.2 Where consent is not given or cannot be given and there is no alternative way to obtain the required information, permission to access the student's account will be sought in the first instance in writing from the appropriate Head of School or Director of Teaching and Learning who will in turn contact the Head of Compliance for authorisation.

5.3.3 Other than in exceptional circumstances, authorisation will normally only be given for access to specific information and not for general access to the account in question. Should general access to the account be required the exact reason for requesting this level of access should be given in writing to the Head of Compliance.

5.3.4 Following receipt of written authorisation from the Head of School / Director of Teaching and Learning the Head of Compliance will contact the IT Helpdesk to facilitate access.

5.3.5 The person authorised to access the account is responsible for ensuring that (unless prior authorisation is given to access the whole account) only the specific authorised information is accessed and that other information is not read or disclosed.

5.3.6 After the necessary information has been retrieved, the password to the absent student's IT account will be reset and the new password will be communicated only to the absent student.

5.4 Access to Staff and Student Accounts - Suspected Illegal Behaviour

5.4.1 Where circumstances brought to the Head of Compliance's attention constitute grounds for reasonable suspicion that a student or member of staff is using the University's IT Facilities for unauthorised activities, and / or the commission or attempted commission of a criminal offence, the Head of Compliance will report such unauthorised use to the police.

5.4.2 In such circumstances the IT account and any associated hardware or peripheral devices should be frozen pending further investigation by the University or the police.

5.5 Access to Student Accounts - Suspected Breach of the University's Regulations

5.5.1 Where there are reasonable grounds to suspect that a breach of the University's regulations has taken place the student will be contacted, where possible, to request consent for access. Where consent is given, the Head of Compliance will record that the student's communications are being accessed.

5.5.2 If it is not appropriate to inform the student or the student is not available to give consent or consent is refused, authorisation should be requested from the Head of Compliance.

5.5.3 The relevant communications should be reviewed by a Disciplinary Officer to assess whether the student has breached the University's Rules and Regulations [and where appropriate a disciplinary investigation should commence].

5.6 Access to Staff Accounts - Suspected Breach of Terms of Contract of Employment

5.6.1 Where there are reasonable grounds to suspect that a member of staff is using the University's IT Facilities in breach of the terms of their contract of employment the member of staff should be contacted, where possible, to request consent for access. Where consent is given, the Head of Compliance will record that the member of staff's communications are being accessed.

5.6.2 If it is not possible to inform the member of staff or the member of staff is not available to give consent or consent is refused or access is required under clause 2.2 above, authorisation will be requested from the Head of Compliance.

5.6.3 The relevant communications will be reviewed by the Director of Human Resources or nominee to assess whether the member of staff has breached the terms of their contract of employment [and where appropriate a disciplinary investigation should commence].

5.6.4 All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000, the Human Rights Act 1998 and the Data Protection Act 1998.

5.7 General Guidance

5.7.1 Any access to the communications of a member of staff, student or authorised user of the University's IT systems will be with as little intrusion and disruption to the communications of third parties that are unconnected to the authorised access as possible.

5.7.2 Any communications collected under this Policy will be treated as confidential and will only be examined by those persons who are so authorised.

5.7.3 Any communications accessed under this Policy will only be retained for as long a period as deemed necessary for the specific purpose and in line with the University's Records Retention Policy.

5.7.4 Any material collected under this Policy will be stored securely and will be labelled accordingly depending on the sensitivity of the material in question. If accessing

communications does not uncover any material/content which would warrant further investigation of the communications of the member of staff, student or authorised user concerned, all material collected will be destroyed after 28 days.

5.7.5 Any person collecting communications under this Policy will ensure that they have continued authorisation to access communications of a member of staff, student or authorised user.

External Username Application

I wish to apply for an external username on the University's IT system. I understand that this username is granted for the sole purpose of Educational use agreed with the University.

General Details

Title:	**Surname:**
First Name:	**Middle Initials:**
Home Institution:	**Address:**
Telephone Number:	
Primary Email Address:	

Hosting Department: _____

Date for Account to expire: _____

I agree to abide by I.T. Services Acceptable Use Policy outlined above.

Signature: _____ **Date:____/____/_____**

B. Authorisation

This section must be signed by your hosting Head of Department / School or your Departmental Administrator.

C. Declaration

I confirm that all information given is correct and that the person named in **Section A** is entitled to use Bangor University computing for the period requested.

Head of Department / School / Departmental Administrator / Computing Officer (delete as appropriate)

Signatory's Name (Block Capitals) _____

Signed: _____ **Date: _____**

IT Services Use Only

Username issued: _____