

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 automatically refer the matter to the Police. The University accepts no liability where such steps are taken.

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 staff, students, and any other person or group granted access to the University's IT Resources.

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 Administrators¹.

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 Head 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.

Information Technology Resources (IT Resources)

For these AUR IT Resources are defined as:

- IT equipment (e.g. computers, printers, university network, 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 ResNet network in halls of residence)
- Software (e.g. email, Microsoft Word)
- Communication/storage of information and any operation involving the manipulation, transmission or viewing of data by electronic means.
- 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

¹ <http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html>

4. Acceptable Use

- 4.1 University IT Resources are provided to facilitate Users education, training, administration or research objectives. The University shall not prevent Users from using the IT Resources for personal non-commercial use for reasonable periods, 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.

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 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 All Users of University IT Resources must ensure that any personal computer, for which they have responsibility and which is attached to the University network (wireless or wired), is adequately protected against viruses through the use of up to date anti-virus software and operating system patches are applied regularly³. All University computers provided for student use have up to date anti-virus software installed, and operating system patch updates enabled.

² <http://www.ja.net/company/policies/aup.html>

³ <http://www.bangor.ac.uk/itservices/sophos/index.php.en?>

- 5.5 All individually allocated cards, usernames and passwords 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. A guidance note is available from IT Services on delegated access to email.
- 5.6 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. Where software is purchased for use on University owned IT equipment, a record of the purchase, and software media (e.g. disks) must be kept.
- 5.7 In the use of IT Resources, Users shall have regard to the University's Intellectual Property Policy⁴ and the intellectual property rights of third parties, especially when downloading, forwarding and using materials which are protected by copyright and/or contain branded materials. For example logos, pictures, text, video files, charts and/or icons.
- 5.8 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.
- 5.9 When University owned IT equipment (e.g. computers/printers) is no longer required, it must be re-used 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).
- 5.10 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.
- 5.11 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 Head of College or Head of School and seek formal authorisation from the Assistant Registrar, Registrar's Office.

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

⁴ Available from the Registrar's Office

- 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. 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 5.4).
- 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 Policy⁵.
- 6.11 Using IT Resources to enter into a legally binding contract unless expressly authorised to do so by the relevant Head of College, School or Central Department.

⁵ Available from the Registrar’s Office

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

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 logs,
- network traffic,
- data stored by Users and images displayed on computers in public access areas,
- 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 prevent or detect a crime,
- To investigate or detect unauthorised use of systems,
- 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 absent from the University (e.g. on sick leave, long-term absence, maternity leave, or 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.

7.5 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 will not exploit or release any material to the University or to a third party without the authorisation of the Assistant Registrar (Registrar's Office) and the receipt of appropriate paperwork. The Assistant Registrar (Registrar's Office) will ensure that relevant legislation (e.g. Data Protection Act) and procedures for release of information are followed. Examples of such releases would be:

- To respond to a request for information supporting investigation by UK 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.
- 7.8 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 necessarily exempt the information from a Data Protection request or a Freedom of Information request.

8. Exit Procedures

When a User leaves the employment of the University, or a student is no longer registered as a current student, or an equivalent 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 Head 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.

Users shall ensure that before they leave, they provide the College/School/Department with the key or code, including all passwords for their IT Resources and that they do not delete any information which the University may require for future use. For example, for auditing purposes or in relation to a Freedom of Information request.

All Users shall also ensure that before they leave they return all University IT Equipment to the 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. General

- 10.1 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.
- 10.2 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.
- 10.3 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.

11. 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:	

Reason for Requiring Computing Access:

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: _____

D. I.T. Services Use Only

Username issued: _____