PRIFYSGOL BANGOR UNIVERSITY

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

Rev	Date	Purpose of Issue/Description of Change	Equality Impact Assessment Completed
1.	8 June 2015	Initial Issue	28th July 2015
2.	19 July 2021	Revised and updated	

Policy Officer	Senior Responsible Officer	Approved By	Date
Head of Governance Services	Chief Operating Officer	Compliance Task Group	19th July 2021

This policy will be reviewed in 3 years

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 2018 (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 organisations / individuals 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 2018.

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

In cases where a member of staff 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 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 get the required information, permission to access the member of staff's account will be sought in the first instance in writing from the appropriate Dean of College, Head of School or Director of Professional Service who will in turn contact the Head of Governance Services 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 be required to the account the exact reason for this level of access should be given in writing to the Head of Governance Services.

5.1.4 Following receipt of written authorisation from the Dean of College, Head of School or Director of Professional Service the Head of Governance Services 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 Member / 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 Member / 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.

5.1.2 Where consent is not given, or cannot be given, and there is no alternative way to get 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 Governance Services.

5.1.3 Following receipt of written authorisation from the Director of Human Resources (or Vice-Chancellor) the Head of Governance Services 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 Governance Services;

- 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.

5.1.4 The final record of information will be placed into the care of the Head of Governance Services who will facilitate access on a business need basis.

5.1.5 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 Staff and Student Accounts - Suspected Illegal Behaviour

5.3.1 Where circumstances brought to the Head of Governance Services' 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 Governance Services will report such unauthorised use to the police.

5.3.2 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.

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

5.4.1 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 Governance Services will record that the student's communications are being accessed.

5.4.2 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 Governance Services.

5.4.3 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 necessary the appropriate disciplinary investigation should commence].

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

5.51 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 Governance Services will record that the member of staff's communications are being accessed.

5.5.2 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 Governance Services.

5.5.3 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 necessary the appropriate disciplinary investigation should commence].

5.5.4 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 2018.

5.6 Forwarding of Emails from Staff / Student or External Accounts

Users' responsibilities in relation to the use of Bangor University IT Resources, including emails, is laid out in the University's Acceptable Use Regulations. IT Resources are provided on condition that they are used for acceptable and authorised purposes only. Occasionally, and in order to deal with incidents where an individual is deemed to be in breach of the University's Acceptable Use Regulations (specifically Section 6: Prohibitions) for example where an individual is harassing or causing distress to a member of staff despite being asked to cease such communications, the University may decide to place a forward on an email address either to a specified individual or to a shared mailbox.

Any such decision would be taken only following the result of discussions between the Head of Governance Services and the relevant Dean of College, Head of School or Director of Professional Service, and would be the subject of regular review by the Head of Governance Services or nominee at least every 28 days.

The individual will be informed that a forwarding process is being put in place, and the reason for the decision. Normally any decision to forward emails away from an intended recipient will be done as part of measures to deal with a potential disciplinary matter, but this would not preclude the University, having risk assessed the situation, to place a forward on an account for other reasons.

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.