User account guidelines

Contents

Introduction

Effective management of user accounts is vital to ensure that correct access rights are granted to University information systems and ensure that this access is restricted to authorised users only.

Scope

This policies covers all information systems used to conduct University business or which are connected to the University network.

Requirements

Access to computing facilities is via individual username and password which allows access to login to central computing services, make use of private file space, run software, access and use email facilities, share and transfer files and gain access to the Internet and the Web.

Accounts are issued for individual use only. For security purposes, users may not share, loan or give away account or password information to any other person. User accounts are to be used only by the assigned user of the account for authorised purposes. Passwords should not be shared, emailed or published. Where it is necessary to record passwords, a secure method must be used (e.g. encrypted password manager software). Default passwords should be changed as soon as practically possible.

Attempting to obtain another user's account password is strictly prohibited. Users are required to change their password if they have reason to believe their account has been compromised in any way. Users are required to take all necessary precautions to prevent unauthorized access to computing resources. Should a business need require the sharing of data and an appropriate route to accomplish this is not clear contact Computing Services to identify one.

Users must be aware of and understand Computing Services AUP before accepting and using an account.

Eligibility

There are four main categories of people who are eligible for access to computing facilities.

- All students who are fully registered on a course at the University
- All staff who are employees of the University
- Staff who are not University employees but who are required, by a particular department, to have access to computing facilities. This third category, known as 'non-payroll staff' for the purposes of this policy, is discussed further below.
- Staff of supported partner institutions such as the Holburne

Non-Payroll Staff

Non-payroll staff must be real individuals. Accounts are not issued to groups, committees, services or similar.

In normal circumstances they will be visiting lecturers or staff who are funded from outside sources, but they could be anyone the department considers in need of computing facilities for University work. Departmental Directory Maintainers, who have administrative responsibilities in the Access Manager system, have the facility to grant access via a non-payroll staff record field.

The department takes full responsibility for these non-payroll staff records and the computer usage of the staff concerned. They must remove the records when the non-payroll staff person leaves or no longer requires computing facilities. The maximum time that a record can exist before review is 12 months.

It is a pre-condition of enjoying the services that follow from registration as a non-payroll member of staff that date of birth is provided to the Directory Maintainer who is setting up the database entry. The purpose of this is to provide a mechanism by which data from different sources can be recognised as such. The date of birth will be treated as confidential and will not be displayed or used for any other purpose.

Collection of Accounts and password management

All students will automatically receive computer accounts at or prior to enrolment.

All other eligible users can go to the Service Desk in the library and ask to be set up with computing facilities. A form of photo identification will be required. If eligibility is confirmed a username and initial password will be assigned.

Exceptionally a new member may be informed of an initial temporary password communicated via a secure channel which should be valid for a limited time period only. This communication should minimise the number of individuals in any communication chain and be made automatically wherever possible.

Temporary Accounts

The use of temporary accounts should be kept to a minimum. Temporary accounts are a support and security overhead for Computing Services. Members of the University of Bath requiring access to University computing facilities should acquire permanent usernames and use these for the duration of their employment or registration.

It is recognised that temporary usernames are required under special circumstances: for example, to provide a service for short courses and community courses.

Computing Services are prepared to create pools of temporary usernames, for a specified period, on the basis that a named individual member of staff is completely responsible for them and the pools of temporary accounts are minimised.

Temporary accounts shall follow the usual username account naming procedures. Temporary staff and student username accounts will, therefore, be differentiated for the purposes of file space allocation, backup, and security.

Individuals holding a Temporary Username are subject to the same terms and conditions, Policies and Regulations as any other computer user at the University. All temporary accounts are full and complete accounts and offer access to the same computing facilities.

A named person for any Department, Faculty or Centre shall be responsible for the management and administration of any temporary accounts in use.

Account Closure

User accounts are subject to closure in the following circumstances:-

- Staff leaving the University - the account is closed on or shortly after the last day of employment. It is expected the individual will arrange for appropriate data held under their account to be made accessible to others for business continuity.
- Staff who change to a new role in the university and need continued access to Computing Services user account privileges between roles can have their accounts and privileges extended when formal notification is given by an appropriate Department Head or representative.
- Dismissal where only university involvement exists - the account is closed immediately. Following the closure, stored data associated with the account can be released with appropriate liaison with Computing Services and appropriate line manager or Head of Department or to an official authority (under normal legal safeguards) if appropriate or required.
- Dismissal where external agencies, in particular the police, are involved - the account is frozen immediately and access disabled.
- Sudden death not requiring investigation - the account is disabled immediately. Data stored under their account can be released following appropriate liaison with Computing Services and appropriate line manager or Head of Department or to other individuals (e.g. next of kin) if appropriate or required.
- Death involving a subsequent investigation - the account is frozen and access disabled immediately. Data stored under their account can be released with appropriate liaison with Computing Services and appropriate line manager or Head of Department or to other individuals (e.g. next of kin) or to an official authority (under normal legal safeguards) if appropriate or required.
- Graduating Students - accounts will be marked for closure at some point within the summer vacation period. An email will be sent notifying the student that the account will close after a grace period of (at least) 30 days. An alumnus account on external services will be opened for them

In all cases of account closure data is archived in line with the normal account cycle and will be recoverable for a period of time if necessary. Frozen accounts are maintained for as long as is required by any investigations.

Document Control Information

Owner	Mark Acres IT Security Manager
Version Number	0.01
Approval Date	
Approved By	
Date of Last review	