IT User Account Policy

1.0 Purpose

This policy defines how user accounts, which provide access to the college computer network and ICT systems, are provisioned and maintained for college staff, students and visitors.

A user account provides access to ICT services including, but not limited to, network, Internet and wireless access, file-storage, email and printing. The usage of these services is provided for educational, academic, and administrative purposes, and must conform to all current college policies and procedures.

2.0 Scope

2.1 This policy applies to all staff, student and visitor accounts created by IT Services for the college, and applies to all information systems managed by, or on behalf of, the college, including those hosted in the cloud; such as Google's G Suite.

2.2 This policy does not apply to privileged accounts such as network and system service accounts which do not belong to a nominated individual but are necessary for the automated operation of the network, applications and connected services.

3.0 Account and Access Control

3.1 Access to computing facilities allows users to log in to the college network, run software, use email and other online services, share and transfer of files and access to the Internet.

3.2 Accounts are issued for individual use only. User accounts are to be used only by the assigned user of the account for authorised purposes. For security, users must not share their account or password with any other person. Please see the Password Policy for additional guidance.

3.3 Users must be aware of and understand the Acceptable Use Policy before accepting and using an account.

3.4 The creation, deletion and changes to user accounts and privileges must be carried out by trained and authorised staff.

3.5 Automated creation of user accounts will be driven by authorised feeder systems including but not restricted to HR and student registration.

3.6 The person enacting any change in a user account must be different from the one authorising/requesting the change.

4.0 Staff Accounts

4.1 A member of staff is entitled to one account and one email address, which will provide access to the network, G Suite and all other ICT systems.

4.2 Staff accounts are automatically created by IT Services when a new member of staff is added to the College's online identity management system by a member of the HR team.

5.0 Student Accounts

5.1 Each student is entitled to one account and one email address, which will provide access to the network, G Suite and other ICT systems.

5.2 Student accounts are automatically created once a student has been enrolled into Pro Solution.

5.3 Student account information must be shared with the student by the teacher. Student account details are available to the teacher in the Pro Solution Control Panel.

5.4 Students requiring a password reset can visit IT Services, Reception or the LRC to have their password reset.

6.0 Temporary Visitor Accounts

6.1 Individuals using a temporary account are subject to the same policies, terms and conditions as any other computer user at the college.

6.2 Temporary accounts shall follow the standard account naming convention.

6.3 All temporary accounts are full and complete accounts and offer access to the same general computing facilities.

6.4 Temporary accounts can be requested directly from IT Services, for a specified period, on the basis that a named individual member of staff is completely responsible for them.

7.0 Departmental and Organisational Accounts

7.1 Departments can request additional departmental or organisational accounts for valid business reasons such as access to a common mailbox or for marketing purposes.

7.2 Account requests must be submitted to IT Services via the online helpdesk by the Department Head or approved organisation delegate.

8.0 Account Closure

User accounts are subject to closure in the following circumstances:

8.1 Closed staff Active Directory and G Suite account names are retained indefinitely so as to avoid re-use of usernames and email addresses.

8.2 Accounts for staff who have left the college and are no longer employed will be automatically closed once the staff member's record is updated by HR in Centime. Closed accounts will lose access rights to all college sites, college systems, online systems and all data.

8.3 Dismissal where only college involvement exists - the account is closed immediately and delegated access can be requested. See section 5.0 below.

8.4 Dismissal where external agencies, in particular the police, are involved - the account is closed immediately and no delegated access is permissible until the conclusion of any investigation or until advised by the Director of HR.

8.5 Sudden death not requiring investigation - the account is closed and delegated access to the account can be requested. See section 5.0 below.

8.6 Death involving a subsequent investigation - the account is closed and no delegated access is permissible to the user's data including files and emails, until the conclusion of any investigation or until advised by the Director of HR.

8.7 Student accounts are automatically closed once the student is no longer enrolled on a valid college course. Closed student accounts lose access to all IT systems, G Suite and data. The account and all data will be deleted as part of the annual clean-up process.

9.0 Departmental and Organisational Accounts

9.1 Departments can request additional departmental or organisational accounts for valid business reasons such as access to a common mailbox or for marketing purposes.

9.2 Additional account requests must be submitted to IT Services via the online helpdesk by the Department Head or approved organisation delegate.

10.0 Delegated Access

10.1 For business continuity, line managers or the Head of department can request delegated access to a closed account.

10.2 Delegated access will be granted for an initial agreed period of time after which access will be revoked unless an extension has been agreed.

10.3 Requests for delegated access to a closed staff account requires the written approval from the Director of HR.

11.0 Managing Privileges

11.1 A user account should have the least privilege that is sufficient for the user to perform their role within the college. Access to information and information systems and services must be driven by business requirements.

11.2 Changes in the privilege of an account must be authorised by a nominated "owner" of the system to which the account affects.

11.3 Line managers and nominated "owners" are responsible for ensuring that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the college.

12.0 Managing Elevated Privileges

12.1 Users whose work requires system administration access will be given elevated privileges in line with their role.

12.2 Line managers are responsible for informing IT Services to adjust the level of privileged access when a member of their team changes roles or no longer has a requirement for privileged access.

13.0 System Service Accounts

13.1 System service accounts are service accounts which do not belong to a nominated user but are used to run a number of automated services and functions. These accounts are created and managed by IT Services in Active Directory.

14.0 Disciplinary Process

14.1 The College reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the College's Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

15.0 Deviations from Policy

15.1 Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the Head of IT Services.