New College Durham

Microsoft 365 Management Policy

Policy Title	**Microsoft 365 Management Policy**
Document Owners	**Academic Registrar / Head of ICT / Vice Principal for Quality Enhancement & Digital Transformation**

Policy Relevant To	**All Staff**
Procedure Effective From	**April 2024**
Next Review Date	**April 2027**

New College Durham is committed to safeguarding and promoting the welfare of children and young people, as well as vulnerable adults, and expects all staff and volunteers to share this commitment.

If you require this document in an alternative format and/or language, please contact records@newdur.ac.uk

We review our policies regularly to update them and to ensure that they are accessible and fair to all. All policies are subject to equality impact assessments which are carried out to determine whether the policy has, or is likely to have, a different impact on those with protected characteristics. We are always keen to hear from anyone who wants to contribute to these impact assessments, and we welcome suggestions for improving the accessibility of fairness of this and all College policies.

To make suggestions or to see further information please contact:

Suzy Taylor
Academic Registrar
records@newdur.ac.uk

Equality Impact Assessed: April 2021
Accessibility Check: April 2021

Contents

1. Scope

This management policy will ensure that responsibilities and the scope of usage for the College's M365 tenant is defined clearly. It will also reflect the requirements of other policies listed in section 3.

This policy will cover the rationale for the definitions and will refer to other relevant College policies.

2. Responsibilities

The **Senior Leadership Team** is responsible for requiring a policy to be in place which establishes the responsibilities and scope of M365 implementation.

The **Executive Director of ICT and Corporate Services** is responsible for providing a strategic direction on the co-ordination of the Intranet Strategy.

The **Head of ICT, Vice Principal for Quality Enhancement & Digital Transformation** and the **Academic Registrar** are responsible for ensuring that the policy scope and definitions are clear and provide consistency when considered alongside other relevant College policies within their areas. They will also be responsible for identifying training requirements to the Training and Development Manager.

The **Training and Development Manager** is responsible for ensuring that training needs analysis is used appropriately to identify required staff training, this will include allocating any costs that would be associated with training or the production of any materials/resources in line with the Lifelong Learning Policy.

The **Information Compliance Co-ordinator** is responsible for the register of sites, annual review of sites, conducting Data Protection Impact Assessments on the various M365 apps, managing the use of metadata, and ensuring guidance is published on the use of M365 in relation to Information Compliance and the management of College records.

The **Vice Principal for Quality Enhancement & Digital Transformation** is responsible for ensuring guidance is published on the use of M365 in relation to teaching and the training of students.

The **Head of ICT** is responsible for ensuring guidance is published on the use of M365 in relation to the administration of the tenancy and the local administration of sites and groups. In addition, the **Head of Systems** will be responsible for managing access for students on the Teams VLE, providing the means to manage Teams, Groups and Sites, and managing the use of metadata.

The **Head of ICT** is responsible for monitoring the Microsoft roadmap and ensuring all potential upgrades to apps are tested and referred for relevant impact assessments prior to rollout.

Site Owners are responsible for the content of their own Intranet sites.

3. Relationship with existing policies and regulations

This policy will ensure clarity in relation to other College Policies:

- Information Security Policy
- Records Management Policy
- VLE Management Policy
- Web and Intranet Management Policy

4. Definitions and Policy Statements

a. A **Tenant** is a single Estate, an organisation can have a number of these if it needs to segregate systems from each other.

A tenant in M365 refers to the full M365 suite attached to a domain which is for New College Durham, newdur.ac.uk. When a tenant is created, it stores all the data for M365 including SharePoint, OneDrive and other applications licensed by the College. This allows all organisational data to sit in the same environment and be moved around within the tenant with ease.

Teams VLE (see point d below) will be separated by standard Teams by name, structure, policy and permissions, however it will reside under the single New College Durham tenant.

b. **SharePoint** is the file store for all M365 applications. For the College, SharePoint sites are set up for each function/department that requires a distinct file store with subordinate ‘document libraries’ used to separate records which have different requirements in terms of permissions or scope. Each function has the opportunity to have an ‘Intranet Site’ which is a place for them to publish information and documents to the rest of the College (see also section e).

SharePoint sites are where records that are required to be kept are held and managed with reference to the Records Management Policy and Manual. The exception is that the Teams VLE holds submitted student assessments.

A Register of Sites is kept, detailing Site Owners and Administrators as well as the method of applying records retention rules to the site.

The process for creating a SP site is detailed on the SharePoint Information site.

c. **Staff Teams** can be created by all staff to facilitate communication and collaboration. It is advised that staff should usually create these Teams around collaborative groups of staff rather than around activities. Activities should be reflected as Channels within the Team.

A Teams Site has an unregistered SharePoint Site attached but it is not expected that staff will use that site for record keeping.

Teams Sites have Site Owners and are managed by an annual review or by an end date.

To request a staff team the member of staff will complete a form hosted on the ICT Intranet site.

Retention of Personal and Teams Chat will be 2 years.

d. **Teams Telephony** – the college telephone system is integrated with Teams. Direct dials are assigned as required and the associated voicemail box is hosted in the cloud. Dial routing and plans, autoattendant functionality, call queues and policies are all created and managed within Microsoft Teams and are the responsibility of the ICT department.

e. **Teams VLE** – Microsoft Teams as a Virtual Learning Environment (VLE) will be for the purpose of structuring, managing and delivering learning activities and content including the tracking and management of online assessments and creating collaborative learning and assessment opportunities for all students in a fully inclusive format. Teams VLE will also serve as a resource centre for staff to engage in professional development.

The Teams VLE is integrated with an anti-plagiarism software:

- To act as a deterrent against plagiarism.
- To provide reports which can help identify occurrences of plagiarism.
- To provide students with a tool to identify and correct possible occurrences of plagiarism in their own work and improve their academic writing.
- To mark the SPAG of each assignment and therefore aid the staff and student in this respect.

f. The **Intranet** will comprise the public facing sites of functions/ departments, these are managed by the relevant department Site Owner. The documents held on the Intranet Sites will need to comply with Accessibility requirements[1] and the structure should be consistent across all sites. (see also section b).

g. **Microsoft OneDrive** is an Internet-based storage platform, a predefined amount of space is allocated to all users with an Office365 licence. Each member of staff will have space in OneDrive to store work in progress and copy documentation. A user’s OneDrive will be deleted with the rest of their account at the appropriate

[1] The Public Sector Bodies (Websites and Mobile Applications) (No 2) Accessibility Regulations 2018

time according to the College fileplan after they leave employment or finish a course.

h. **Microsoft Exchange** is the software that runs the email and calendar functionality that is presented by MS Outlook or other email application. College Data will be stored on the MS Cloud, enabling functionality within M365.

i. **Compliance Centre** is the functionality that is used by Academic Registry and ICT to run maintenance and searches on files within the tenancy. It will be used to compile Information Compliance Request responses and to enable content search on request for other business purposes. Academic Registry will use this for disposition review and management for content and metadata where retention labels or policies are applied at document and site level. It will also be used to demonstrate regulatory compliance.

   Additionally, the compliance centre monitors for any data being shared by staff on the various Office platforms and attempts to block any potential data breach. The systems will attempt to stop inappropriate disclosures of personal, financial and other confidential data.

j. **Management of Teams, Groups and Sites** – Retention and archiving of these will be managed via the group expiration policy. The owner of a group/team/site will be contacted after the group/team/site is inactive for 1 year and asked whether to keep their group/team/site. They can either click to keep alive or ignore for it to be archived. If any documents need to be retained once a site is no longer in use, the users of the site can copy the files to another SharePoint site. The Information Compliance Co-ordinator will review the list of deleted sites every 2 months and contacting the owner(s), as appropriate, to check that they have retained copies of files they may need that have not passed their retention period. If a site has no owner it will be assigned to the Records account.

   As part of the existing process to log staff leavers the Information Compliance Co-ordinator will check the log of SharePoint sites and where the staff member is listed as a group owner, will ensure that a new owner is assigned to the group, following discussion with the department concerned.

k. **Management of Metadata** will be co-ordinated by Academic Registry and ICT so that consistency is applied across the tenant.

   The key metadata types identified across the tenant will include Staff ID and Student ID and any identifier that is used to aggregate records (examples might be asset reference, invoice number, course ID). Any identifier that is vital to ensure effective records are maintained should be selected from a lookup or integrated list that pulls the identifier from the system where the primary record is held. Users should not free type. This enables consistent search across the tenant.

l. **System Owner / Site Owner** - The IS Policy requires there to be a System Owner for each College System. For the M365 tenancy the overall System Owner is the Head of ICT.

For the Teams VLE the Vice Principal for Quality Enhancement & Digital Transformation will be the owner.

For each SP Site or Staff Team the Owner is listed in the relevant register. It is likely this will be a senior member of the department. This person is responsible for ensuring permissions are adequate and maintaining compliance with the Information Security Policy. This person should be the Data Owner (person who holds managerial responsibility for the data held in the site) and will usually be responsible for ensuring records retention rules can be applied.

m. **External Access** will be managed by the Site Owners applying the relevant access.

External Access can be granted by any member of staff. This will enable external people to attend meetings.

Guest Access can only be granted by Site Owners as they are responsible for permissions across their site. This should be done in the context of the Information Security Policy and with due regard for the protection of confidential and personal records.

The following are examples of where these access types might be used:

- External Examiners (Guest)
- Employers (Guest)
- Consultant (External)
- Inspector or Auditor (Guest)
- Partner Organisations (Guest)
- Potential Student and Employees (External)
- Guest Speakers (External)

5. Students

Students will have an M365 account for use whilst they study at the College. They will be given access to the Teams VLE and will have a College email address and a OneDrive to store their work.

Training will be provided by staff who would usually be expected to help students adapt to new technologies.

Students will be expected to use their College email to communicate with the College. The College will send any communications relevant to their study to this email and the students are expected to ensure they check their inboxes regularly.

The students indicate their commitment to ensuring they use College ICT systems and equipment correctly during their enrolment.

6. Staff

Staff will have an M365 account for use whilst they are employed by the College. They will be given access to the Staff Teams and teaching staff will have access to relevant areas of the Teams VLE. They will have a College email address and a OneDrive to store their work. Staff will also have access to relevant SharePoint sites.

All staff as part of their induction will receive training on M365. This will be further supported by training provided by the IT Training Officer and Lead Practitioner e-Learning.

Staff indicate their commitment to ensuring they use College ICT systems and equipment correctly as part of their employee contract.

7. Third Parties

Third parties who are assigned College M365 accounts will indicate their commitment to ensuring they use College ICT systems and equipment correctly when their account is assigned.

8. Information Security

The Information Compliance Co-ordinator will maintain a Data Protection Impact Assessment to ensure any changes to functionality are assessed for their impact on Personal Data. The Head of ICT will ensure an Information Security Impact Assessment is also maintained as required by the College's Information Security Policy.

9. Review

This policy will be reviewed every 3 years or as necessary to ensure it is fit for purpose.