



SOFTWARE LICENCE POLICY

1 Introduction

1.1 Purpose of Policy /Procedures or Guidelines

The aim of this policy is to clarify roles and responsibilities in relation to the installation and management of software on University IT facilities and to outline procedures to ensure that software licences within the University are effectively managed and recorded.

1.2 Scope

This policy applies to all staff and students at the Manchester Metropolitan University.

1.3 Roles & Responsibilities

The policy will be implemented by IT Services.

2 Policy/Procedure/Guidelines

2.1 Software Installation Policy

- IT Services shall assess the impact of installing non-standard software at the request of users, provided that a valid license is produced
- Installation of non-standard software will be carried out by IT Services, provided that the installation does not result in any adverse impact on the operation of the standard operating platform
- Details of all valid licenses are recorded by IT Services and held in a central, secure database
- If specialist, non-standard software is required staff should raise a call with the IT Helpline and a member of IT staff will discuss their requirements with them
- IT Services will use a system to monitor and record the usage of all installed software to ensure no illegally obtained software or software with an expired license can be used on our systems

2.2 Freeware policy

- The user is responsible for ensuring that any freeware they request to be installed is legally designated as freeware for use in the work environment
- Any freeware identified for installation should be designated as such by the GNU GPL licence or recognised equivalent



2.3 Administrator Rights to User Devices

- Default setting is that users are not given Administrator rights
- Administrator rights shall be granted if the relevant Head of Department supports a credible business case for the user
- User with admin rights is responsible for ensuring all software installed on the device is legally licensed for use in the work environment
- Devices controlled by users with admin rights shall be audited twice yearly
- If illegal software is discovered as a result of these audits, admin rights will be revoked and the user may be subject to further disciplinary action in accordance with MMU policies and procedures
- IT Services shall keep records of all users who are granted admin rights, together with details of all the devices they use.

4 Version Number and Approval Dates

Version	V3.1	Author Name & Job Title	James Woodward Client Services Manager
Approved Date	August 2013	Approved by: (Board/Committee)	Mo Din Head of IT Services
Date for Review:	August 2015		