

Policies Document

Cambridge Virtual Learning Environment (VLE)

Terms and Conditions

Introduction

Moodle is a Virtual Learning Environment (“VLE”) which offers file sharing and communication tools to users. Cambridge University provides these services subject to the following rules and guidelines.

These guidelines should be used in conjunction with the following University policies which can be found on the University web site:

- IT Security Policy
- Acceptable Use Policy
- Procedures relating to misconduct
- Accessibility Policy
- Privacy Policy
- Data protection Policy
- Freedom of Information Policy

In the event of any conflict between this document and any University Policy the terms in the policy will govern. Any questions regarding Moodle usage can be directed to the Moodle Manager.

Use of Moodle

When using Moodle and connecting services, users must

- Respect the rights of others.
- Remember to logout at the end of each session.
- Comply with current and future legislation including:
 - The Data Protection Act 1998
 - Copyright, Designs & Patents Act 1988
 - Computer Misuse Act 1990
 - Telecommunications Act 1984
 - Protection from Harassment Act 1997

Each user (lecturer, supervisor, learner or guest) is responsible for ensuring that their use of Moodle complies with University policies and this document.

By using our Moodle services users agree to be bound by these terms, which shall take effect immediately on their first use. If users do not agree to be bound by all the following terms they should cease using Moodle and notify MISD.

The University may revise these terms without notice by posting the latest version of this document onto Moodle. A user's continued use of Moodle will be deemed acceptance of the updated terms or amendments.

Users accessing Moodle from non- University owned equipment (such as mobile phones or personal laptops) and users accessing Moodle from outside University or College premises (such as their home or workplace) are bound by the same conditions of use.

In accordance with the University Acceptable Use Policy, use of Moodle must be for the purpose of teaching, training, research, coursework, associated administration or other authorised use.

Security

Access to course information and resources on Moodle are controlled by user permissions. Users should log into Moodle with their own network user account and never allow another user to access Moodle under their network account.

If an area on Moodle is protected by an Enrolment Key (a password required to gain access) that is set by the lecturer or supervisor learners should never disclose the enrolment key to allow access by an unauthorised user.

Users should never attempt to access any protected Moodle area unless they are a member of the course and have been given permission to do so by the course lecturer or supervisor.

Activities on Moodle are fully audited. Records are kept of when users access courses and resources along with a log of all communications such as forum posts, assignment submissions, etc. These records are available to lecturers or supervisors for course evidence, but may also be used as a point of reference for any matters arising, such as accounts of harassment, bullying or the transmitting of inappropriate material.

Users should not post personal or sensitive information to any part of Moodle including to their profile, blogs, or any course activities. Information sent through Moodle may be read by third parties.

When lecturers or supervisors place information onto Moodle they are acknowledging that they are making it available for download, and therefore we cannot guarantee that such resources will not be seen by/distributed to third parties.

Often lecturers or supervisors will place links to useful websites on Moodle to help learners with their research. The University cannot accept any responsibility for the contents of external sites.

Access to Moodle will be withdrawn when a user is no longer employed by/studying at the University.

Content

Course lecturers or supervisors are responsible for ensuring that the learning materials added to their areas does not infringe confidentiality, copyright or the intellectual property rights of others (including colleagues).

Course lecturers or supervisors should not upload any materials which would breach the University's acceptable usage policies (such as illegal or obscene content) or add links to any web pages that host such material.

Learners taking part in online course activities (including assignment submission, chat rooms, forums, etc.) are prohibited from transmitting any words or pictures which are libellous, insulting, and abusive or would otherwise contravene the University's codes of conduct.

All work submitted electronically by learners should be their own. Copying others work, cheating, collusion, plagiarism and attempting to obtain unfair assessment advantages are in violation of the University policies.

Course lecturers or supervisors are responsible for supervising their Moodle areas and ensuring that any violations of University policies are dealt with. Any violations of policies identified by learners should be made to their lecturer or supervisor in the first instance.

Moodle areas should reflect current learning provision. Once an area has been created for a lecturer or supervisor it is their responsibility for ensuring it remains up-to-date.

Moodle areas may be removed without warning if:

- The lecturer or supervisor has not accessed the area since it was created
- No resources and/or activities have been added to the area
- The area has no recent access by learners
- The area is inappropriately visible in the hierarchy.

Where a course area has multiple lecturers or supervisors then arrangements should be made by the lecturers or supervisors team to ensure that they work together collaboratively. The University cannot accept any responsibility where a lecturer or supervisor makes changes to files or settings without informing their colleagues.

Moodle contains documents created with a variety of software. Where possible we encourage lecturers or supervisors to upload resources in commonly used formats (such as Microsoft Office) to offer wider compatibility. The University cannot support learners with problems opening files externally if they are caused by incompatible software and/or hardware.

Many files on Moodle (such as videos) are quite large and best viewed over the University network. The University cannot guarantee quality of performance or be responsible for connection issues when downloading these materials externally.

Data Protection

Users of Moodle must agree to:

- Look after their own username and password. They must not share their password with anyone else and must not use the username and password of other users
- Keep physical access to Moodle secure. For example, they must not login to Moodle and then leave their computer unattended
- Not attempt to gain unauthorised access to any part of Moodle
- Not post material which contains viruses or other programs which may disrupt the University's systems
- Not upload private, confidential or sensitive material unless this is authorised
- Keep their own data up-to-date and secure
- Understand that the University will not take responsibility for any loss of information, which has been posted on Moodle, once users cease to be formally associated with the University.

Access logs

Access to this course is logged and the information recorded about course usage is available to the course managers. This information includes which users have visited the course, when they visited and what they have looked at. These statistics are monitored and may be used:

- to provide information on course usage
- as part of our student assessment

If you have any concerns, please contact the course manager.

Data storage limitations

Moodle is a platform for making files and resources available to learners throughout their course. It should not be used as a general storage area.

Files that are not required for the delivery of a course should be stored in a staff network area or on a user's own disks. Where collaboration is required between staff then an appropriate network shared area should be used.

Staff should always keep original copies of work they upload onto Moodle. The University accepts no liability for lost or corrupt data that has been stored on Moodle by staff or learners.

Whilst the server is routinely backed up for the purposes of disaster recovery it is the responsibility of users to ensure that they have copies of any important data, including uploaded resources, submitted assignments, etc.

All learner data and submitted work are purged from the server at the end of the summer term ready for the next academic year. Staff should ensure that they have copied off any submitted assignments, feedback, grades, forum posts, quiz scores, etc. that they need to keep as evidence.

Where course information needs to be retained, or where learners will be active through the summer period staff should consult (in advance) with the Moodle Coordinator to ensure data is not lost.

University computers are routinely virus scanned but the University cannot guarantee that all files transmitted through Moodle will be virus free. Users accessing Moodle from home should ensure that they have adequate virus protection on their computer to help prevent their infection or distribution of viruses.

Staff should not use Moodle as a tool to distribute software applications to learners (except where it has been created as part of a programming course).

Disciplinary Action

Should a user contravene these terms of use or any other College Policy related to the use of Moodle, the offence will be logged and appropriate action will be taken, from a temporary restriction of services up to and including permanent removal of services and further disciplinary procedures.

Information about us

Moodle is operated by the University of Cambridge (the 'University' or 'we' or 'us') whose registered address is The Old Schools, Trinity Lane, Cambridge, United Kingdom CB2 1TN