Student Computing Policy
Updated March 2024

Contents

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Alternative format of this Policy

If you require the Student Computing Policy in an alternative format, contact your Student Support Team or Apprenticeship Enrolment and Support Team. Research degree students should contact the Research Degrees Office at research-degrees-office@open.ac.uk. Microcredential students studying via FutureLearn should contact mc.support@futurelearn.com. If you are studying a Microcredential via The Open University's Virtual Learning Environment should contact your Team. See also section 'Contacting us' below.

Summary of policy

The Open University Student Computing Policy sets out the ways you are expected to use Open University computing services.

This policy will help you to understand your responsibilities when using a computer to support your studies, including:

- participation in online activities

- publication of materials using Open University supplied services

- communicating electronically

- the protection of Open University computer systems, services, and networks

- expected standards of behaviour

- the consequences of breaching this policy.

The use of social media is covered by our Social Media Policy.

If you do not comply with the Open University Student Computing Policy we may bring disciplinary action against you under the Code of Practice for Student Discipline. Section 2 of the code gives details of what constitutes an offence while Section 3 outlines any consequences of being found to commit an offence.

If you have any queries about this policy, please see 'Contacting us' below.

For questions about your use of social media when discussing your studies or The Open University, contact the Social Media Engagement Team at social-media@open.ac.uk.

Scope

What this policy covers

This policy applies to you if you have permission to sign into Open University websites and systems and are not a member of staff. If you are both a member of staff and a student or learner, this policy only applies to you when you are signed in as a student or learner. This includes if you are studying a Microcredential that is delivered either on The Open University Virtual Learning Environment (VLE) or on the FutureLearn platform.

For students studying at Subsidiary Institutions of The Open University, this policy applies to you only while using our computing services, such as Library Services. When using computing services provided by a Subsidiary Institution you will be subject to the Computing Policy of the Subsidiary Institution. If you are unsure, check the URL (site address) which should indicate whose site it is. Open University sites end with @open.ac.uk, for example.

Throughout this policy, when we refer to 'study' or 'study materials' we include modules as well as other forms of Open University study (e.g., Microcredentials, short courses and vocational qualifications).

Throughout this policy, "we/us/our" refers to The Open University, and "you/your" refers to any Student or learner who falls under the scope of the policy.

Vocational Qualification (VQ) learners have access to student policy information and the [Computing Helpdesk.](#) They can study from outside the UK and can obtain materials in alternative formats but may not have access to some of the other facilities mentioned in this policy, including access to StudentHome and an Open University email address.

This Policy may be updated throughout the year to correct errors, improve clarity or accessibility, or to reflect changes in legal or regulatory requirements.

What this policy does not cover

This policy does not apply to you if:

- you do not have Open University sign-in credentials, including VQ students

- you are a member of Open University staff, except if you are signed in as a student or learner.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Note that Students in secure environments and those with legal licence restrictions, conditions or orders may have limited access to computing services and should also refer to our Students in Secure Environments Policy or our policy on Supporting students subject to legal licence, restriction, condition or orders

The Open University Student Charter Values

The Student Charter was developed in partnership by The Open University and the OU Students Association. It is a declaration of our shared values and the commitments we make to each other. This policy has been developed with the Student Charter values as its foundation.

Introduction

This policy sets out how you should use an internet connected computer to study with us and use our computing services. In addition, the policy explains what your responsibilities are and information about how we can support you It also explains how we will communicate with you and how you should communicate with others when online. Terms that may be unfamiliar are explained in the glossary. There are no specific issues related to equality or diversity, but the policy does cover possible breeches of data protection. It also covers the impact of legislation.

Policy

1. Purpose

This policy sets out to ensure that students understand the rules and responsibilities which must be followed when using a computer to access our computing services. Our responsibility is to protect our services and other students and staff and to ensure that we are compliant with the relevant regulators and legislation.

2. Using a computer for your studies

2.1 What you will need a computer for

To study with us you need the use of a computer with internet broadband access and some basic computer skills. To check the required standard, see our Computing Skills page.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

You will use your computer to access online module materials, participate in forums, publish information (for example via blogs and ePortfolio), find student support details, view your personal record, undertake and submit assessments, book and attend tutorials and to contact us.

2.2   Computing requirements for study

There are minimum requirements for the specification of computers and internet connections that apply to all modules, for more help see the Computing environment section in the Computing Guide. In addition, you should check the 'Computing Requirements' section of the module description on the online prospectus (if applicable) for any requirements specific to the module that you wish to study. If you wish to print out any of the online module materials, you will need access to a suitable printer. Students with disabilities should visit the Help Centre for information about computer related support.

Since technology is developing rapidly, the general specifications may change over the time that you study with us, so please check these each time you consider studying a new module, and contact us if you need support.

2.3   Study outside the UK

The following clauses only apply to individuals planning to study with The Open University when resident (temporarily or permanently) outside of the UK and Ireland.

2.3.1   To be able to access study materials and learning events via the digital services provided by The Open University, you will need to sign into your student account: this will enable you to engage with your studies. In most cases, the ability to sign into your student account and use our digital services will be fully accessible. However, in a small number of geographical locations (please see The Open University guidance "Signing in from outside of the UK"), access may be restricted or not be permissible without use of a VPN (Virtual Private Network).

2.3.2   If you are planning to study with us from outside the UK and Ireland, please see "Signing in from outside of the UK" for information about current restrictions. These restrictions may impact upon your continued registration with The Open University, in line with our Conditions of Registration, Conditions of Registration (Short Courses), Conditions of Registration for Apprentices), Conditions of Registration (Microcredentials hosted on the Virtual Learning Environment (VLE)) or Conditions

| Version number: 3.0 | Approved by: Delegate of Director, Academic Services. |
| Effective from: August 2024 | Date for review: March 2025 |

of Registration for Degree Holder Entry Programme (DHEP), as appropriate. You should contact us if you have any concerns (see Contacting us' below)

2.3.3   If you are studying in, or intend to travel to, a country that currently has restrictions on access and requires a VPN, please see the relevant Conditions of Registration for information about your obligations as a student and our obligations to you.

3.   Computing support

3.1   Once you have registered with us, you will have access to help and advice from a dedicated computing helpdesk, which you can contact via phone, email or (when available) webchat, the Help Centre and the Library.

3.2   If you require additional support to use IT equipment because of a disability or additional need or want help or information about using a computer, go to the Help Centre accessibility pages. There is also an accessibility guide to using a computer for study in the Open University Computing Guide. If you require these resources in Alternative Formats please contact us (link).

3.3   You should be aware of how to take care of your health and safety when you are working on a computer. Further information can be found in the 'Using a computer and your wellbeing' section in the Help Centre.

3.4   Please report content on websites or online services provided by us that you are concerned about by Contacting us. If you are concerned about content that appears on social media platforms, please refer to 'the Monitoring and reporting behaviour' section in our social media policy. See also How to report bullying and harassment on social media.

3.5   Welsh language: you have a right to submit written work in Welsh. To assist with this, you are able to request access to Cysill, a Welsh-language spell-checker from the computing helpdesk to request this.

4.   Your Open University computing account

4.1   Your Open University Computer Username (OUCU) and password

4.1.1   We will give you a secure Open University computing account when you register. You can access this account using an Open University Computer Username

| Version number: 3.0 | Approved by: Delegate of Director, Academic Services. |
| Effective from: August 2024 | Date for review: March 2025 |

(OUCU) and password that we will provide. This will give you access to the Open University computing services you need for your studies. You should not use your account for any business or personal purposes.

4.1.2   You can set a different username, but it should remain a true representation of your real name so that your tutor can identify you.

4.1.3   You will breach this policy if your selected username may be considered offensive.

4.1.4   Your password must be in line with accepted good practice. The Help Centre has advice on choosing suitable passwords.

4.1.5   You must not share the contact details of any member of the University, student or staff, including computer username and email address, without their express permission. See also section 10

4.1.6   Always ensure that you keep copies of any work you submit to us online in case there are technical problems, and you need to resubmit the work. You may need evidence of any technical failure if you are unable to submit work and want to make a Special Circumstance claim. For more details, see our Special Circumstances policy.

4.2   Keeping your account secure

4.2.1   You should always keep your account secure and confidential; your account details should not be accessible to anyone else. Please visit the Help Centre's 'Safe and secure computing' pages for up-to-date information about keeping your account secure. If you have an advocate who acts on your behalf, you must not disclose your account details to them; see section 1.9 in our Advocacy Policy. This policy is viewable by advocates and doesn't need an account.

4.2.2   If you think the security of your Open University computing account has been compromised, for example if somebody else knows your password, you must notify the University Computing Helpdesk by completing the Helpdesk contact form or calling +44 (0)1908 653972 as soon as possible. You may be held responsible for fraudulent activity if someone else accesses your account because they have been given your sign on credentials and you haven't informed us.

| Version number: 3.0 | Approved by: Delegate of Director, Academic Services. |
| Effective from: August 2024 | Date for review: March 2025 |

Page 8 of 19

5. Sharing information in online activities

5.1 Display of personal information

Your Open University computing account enables you to participate in online activities, which may include compulsory activities as part of your studies, such as participating in module forums. In most cases, when you participate in these activities, your name, preferred email address, your Open University Computer Username (OUCU) and the content you contribute, will be displayed online to Students and Open University staff who have a need to see the information concerned.

If you want others to know a bit about you when you contribute to forums, you will be able to update your 'online appearance profile', for example so that it shows your social media ID and interests. Your online appearance profile can be accessed from various locations. Full details are provided in the Profile section of the Open University Computing Guide.

5.2 Retention of messages

Messages sent or received through Open University systems form part of the administrative records of The Open University and will be held on our Customer Relationship Management system to help us support you. The Student Privacy Notice sets out how we use your personal data.

5.3 Sharing personal information

When working online, you should carefully consider the information that you are sharing with others. For example, do not share personal information such as your home address or bank details. More information is available in the 'Conduct when communicating online' section of the Open University Computing Guide.

6. Online communication

6.1 Contacting you by email

6.1.1   You must provide us with a valid email address, which we will use to correspond with you. You must inform us of any changes to your preferred email address by updating your personal profile on StudentHome. Students studying modules or working towards a qualification will be provided with an Open University email address before their module

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

starts, but you are not obliged to use this as your contact email address. For more information see the Your OU email address section in the Help Centre.

6.1.2   We will use your preferred email address to communicate with you, and so you need to read and respond to these messages by any deadline given. We do not accept liability for messages that were not received, for example because your email was not working, you changed your email address without informing us, your mailbox was full, or because a junk or clutter filter meant it was removed from your inbox.

6.1.3   If you are receiving marketing messages, you can opt-out or update your preferences in your StudentHome profile. The Student Privacy notice sets out how we use your personal data.

6.2   Communicating with you by the Bulletin Board

We use email for messages relating to your studies where you need to take personal action, for example, to meet a deadline. In addition, you will also find more general 'bulletin board' messages on StudentHome and on your module website. It is your responsibility to regularly check these. Note that you can opt out of some messages, for example, those that are marketing related.

6.3   Communicating with you through your study websites

We will communicate with you through your study website, forums, and news feeds and so you should check your study website regularly.

6.4   Conduct when communicating online

The Student Charter sets out the responsibilities we have to each other as members of the Open University community. In addition, the principles of communicating with other students in Open University collaborative spaces are outlined in the 'Conduct when communicating online' section of the Open University Computing Guide. When using social media as a student, you must adhere to the Social Media Policy. See also section 10, Non-compliance, below.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

7. Protection of Open University computer systems

7.1 Keeping your computer and our systems safe

Working online may expose both you and our computer systems to threats from outside the Open University, unless you take suitable precautions against malicious software (for example, computer viruses) that may jeopardise the integrity, performance or reliability of our computing services.

To reduce the risks of such threats, you must ensure that you:

a) Have up to date virus protection software and do not forward junk mail to others or encourage others to do so, since malicious software is often spread this way

b) Treat email attachments with caution, as they may carry viruses or other malicious software. If in doubt, do not open suspicious emails. For further information, please see our guide to Safe and Secure Computing.

c) Avoid hacking sites or downloading hacking or evidence eliminating software. Do not attempt to hack into Open University computer users' accounts or Open University systems.

d) Do not intentionally visit internet sites that are likely to contain obscene, racist, hateful or material likely to be seen as offensive, nor download or share such material via our systems.

e) While your right to freedom of speech is protected, you should not publish any content, for example, via blogs, forum contributions, ePortfolios and so on, that might contain material that is defamatory, obscene, discriminatory, illegal, incites hatred or could damage our reputation or breach copyright of The Open University or any other person or organisation.

f) Do not do anything that might result in sustained high-volume traffic to our network, for example by sending emails to large numbers of addresses, as this might prevent others from accessing the network. We may block or quarantine any email or online posts if we identify it as a potential threat to our network.

g) Your Open University email address is intended to support your study. Incidental and occasional personal use is permitted, but shouldn't be used for regular personal activities, such as online shopping.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

h) If you think you may have compromised our network, you must contact the Computing Helpdesk immediately (see Contact us) below. We may investigate any breach or potential breach by accessing all relevant records and other evidence.

Further information on safe computing can be found in the 'Safe Computing' section of the Open University Computing Guide and the 'Safe and secure computing' section of the Help Centre.

7.2 Blocking content

We may delete or hide any item that you publish via our network and systems, such as forum posts, blogs or ePortfolios, where we believe they do not meet this policy. Further information can be found in the 'Conduct when communicating online' section of the Open University Computing Guide.

8. Standards of behaviour

8.1 Acceptable standards

When using our computer services, you should observe the standards of behaviour as outlined below:

a) You should only use our computing services for the purpose of your study with us unless we have agreed otherwise. This includes any online storage space provided as part of your studies, such as the ePortfolio system or Microsoft 365, which should only be used for storing items related to your studies and will cease to be available when you stop studying.

b) When you study with us, you agree to follow any licensing agreements for software provided.

c) You should not send or publish offensive, obscene, abusive, libellous, defamatory or harassing material or anything via our computing services that might damage our reputation.

d) You should not present your own opinions or other information from your own sources as if they are those of The Open University or made on our behalf.

e) Any software, website content, study materials or other information provided by us must not be copied for non-study use without prior permission from us or any relevant third-party supplier.

| Version number: 3.0 | Approved by: Delegate of Director, Academic Services. |
| Effective from: August 2024 | Date for review: March 2025 |

You should not share online any questions relating to assessment nor any completed assessments. The only exception is where prior consent has been given by The Open University in writing. For further details, please see section 3.3, Enabling Plagiarism, in our Academic Conduct Policy.

f) The unauthorised use of generative Artificial Intelligence and automated tools is covered in section 3.6 of the Academic Conduct Policy.

If you realise you have unintentionally enacted any of (a) to (f) above, you should determine if you can undo what you have done, for example, delete a forum or message post. Otherwise, you should contact us and explain the situation immediately (see 'Contacting us' below).

g) You should comply with The Copyright, Designs and Patents Act 1998. This means that you should not infringe copyright relating to materials and software provided by us. This includes storing copies of copyright material on any online space provided as part of your studies (for example the ePortfolio system).

h) You agree to follow the requirements of the Computer Misuse Act (1990), the Criminal Justice and Public Order Act 1994, data protection legislation and other relevant Acts.

i) You agree to abide by the policies of our partners where you are using their services or facilities through us. In these cases, you will be subject to the regulations of the institution you are accessing the services from. In addition, cloud services may also have policies for users of their services.

j) Users accessing our computing services from outside the UK must ensure that they abide by all local laws, e.g., the use of a VPN to connect to our network. You should ensure that you have the consent of the owner of the computer/network owner, for example if you are accessing our services from work.

k) You should not promote any product or service via our computing services for which you are paid either financially or in kind. See also section 2.1 of the Social Media Policy

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Page 13 of 19

9.   Monitoring

9.1   In exceptional circumstances, we may use records of your study activity and your contact with us to carry out our work or meet our legal obligations. The Student Privacy Notice describes how we will manage these records.

9.2   For security and maintenance purposes, authorised individuals within The Open University's central IT teams may monitor online services, systems and network traffic at any time to ensure compliance with this policy, other security policies, and the effective operation of The Open University's systems.

9.3   As an institution of higher education, we have a statutory duty to prevent people being drawn into terrorism. If the use of our computer equipment, network, or online services and systems gives rise to a concern that a person may be at risk, this may result in action being taken in accordance with the Open University Prevent Principles.

10.   Non-Compliance

10.1   Any breach of this policy may undermine the effective running of The Open University and its ability to meet its duties and legal obligations.

10.2   If you do not manage your Open University computing account as stated in Section 4.1 above, it may adversely affect your learning experience. For more serious breaches of the policy, such as those related to security (section 3.2) or standards of behaviour (section 7), action may be taken under the Code of Practice for Student Discipline. If your conduct and/or actions(s) are also unlawful, we may inform the appropriate authorities. We may also have a statutory obligation to inform other internal departments such as the Safeguarding Referrals Team or the Prevent Coordinator of specific behaviours of concern and may also need to share relevant information with external parties.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Contacting us

Please use the contacts page to contact your Student Support Team or Apprenticeship Enrolment and Support Team. This also provides contact details for the computing Helpdesk.

Research degree students should contact the Research Degrees Office at research-degrees-office@open.ac.uk.

Commitment to Equality, Diversity and Inclusion at The Open University

Policies are inclusive of all Open University Students, Learners, Enquirers and Alumni, regardless of age, civil status, dependency or caring status, care experience, disability, family status, gender, gender identity, gender reassignment, marital status, marriage and civil partnerships, membership of the Traveller community, political opinion, pregnancy and maternity, race, religion or belief, socio-economic background, sex, sexual orientation or trades union membership status.

Safe Space Reporting

The Open University is committed to creating a diverse and inclusive environment in which everyone feels safe and is treated with dignity and respect. Unlawful discrimination of any kind across our University will not be tolerated. Safe Space Reporting is available through an online tool through which staff, students, learners and visitors are encouraged to report incidents of assault, bullying, harassment, hate crime, or sexual harassment. It also provides information about what you can do if these incidents happen to you, or to someone you know, and where you can find support.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Glossary

Virus protection software

Virus protection software is designed to detect and remove viruses and other kinds of malicious software from your computer or laptop. Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them.

Blog

A blog, short for weblog, is a website or web page, typically one run by an individual or small group, which is written in an informal or conversational style.

Bulletin Board

An electronic notice board, accessed via StudentHome or module website, where the University will post study-related topics that might interest you.

Computing helpdesk

A service to help you support you with study related computing queries. For more details, see Asking for help with IT in the Help Centre.

Computing Services

All computer systems provided by The Open University and its third-party suppliers that we to teach and support students and learners. This includes software, websites, hosted services and the associated IT and telecommunication hardware covering the transmission, storage, organisation, presentation, generation, processing or analysis of data and information in electronic format over our network or those of our suppliers.

Customer Relationship Management system

The administrative student record system that we use when you contact us. This allows us to keep a record of email and telephone conversation with you along with a note of any action we have taken in response.

ePortfolio

An electronic, curated collection of material designed to provide evidence of your developing professional competence.

Hacking

The gaining of unauthorised access to data in a system or individual computer.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Junk email

Unsolicited and usually unwanted messages sent in bulk by email using mailing lists,

Open University Computer Username (OUCU)

In most cases, when you register to study with us you will be issued with an Open University Computer Username (OUCU) that, along with your password, will allow you to sign on to our computing services.

Preferred email address

This is the email address provided by you that we will use to communicate with you about your studies.

Prevent (anti-terrorism)

As part of the UK Government's strategy to reduce terrorism, the Counter-Terrorism and Security Act 2015 introduced new measures aimed at responding to the risk of terrorism and radicalisation. Under the Act, we must show 'due regard to the need to prevent people from being drawn into terrorism'.

Social media

For the purposes of this policy, 'social media' is defined as websites and online applications that enable users to create and share content, and/or participate in social networking. These social media tools enable users to share ideas, opinions, knowledge and interests and use of them includes posting, commenting, instant messaging and sharing links, images and files.

Study websites

These are module- or qualification-related websites that are provided to support you with your studies and include teaching material, study timetable and so on. You will only have access to these websites while you are an active student on that qualification or module.

Virtual Private Network (VPN)

A Virtual Private Network (VPN) is an encrypted network connection that allows remote users to securely access an organisation's services. This means that the security of the data is ensured even though the network itself may not be trusted.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Page 17 of 19

Related Documentation

Refer to the following documentation in conjunction with this document:

- [Advocacy Policy](#)

- [Code of Practice for Student Discipline](#)

- [Academic Conduct Policy](#)

- [Student Privacy Notice](#)

- [Safeguarding - Ensuring the Safety of Children and Vulnerable/Protected Adults](#)

- [Dignity and Respect Policy](#)

- [Prevent Principles](#)

- [Social Media Policy](#)

- [Students in secure environments or Studying with an unspent criminal conviction](#)

- [Computing help (Help Centre)](#)

- [Open University Computing Guide (available once registered),](#)

Additional support

- [Being digital: skills for life online](#) (Open University Library)

- [Digital skills: succeeding in a digital world](#) (OpenLearn free course)

- [Social Media Toolkit](#)

- [How to report bullying and harassment on social media](#) (via [Dignity and Respect Policy)](#)

- [A template for community guidelines](#) (for student group administrators)

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025

Summary of significant changes since last version

The student computing policy has been significantly rewritten to ensure that the policy reflects current practices, is more comprehensive and easier to understand. The main changes are:

a)   A 'purpose' section has been added to the top of the main policy to ensure consistency with our other policies and some of the sections have been moved around for the same reason.

b)   Similarly, the 'Commitment to Equality, diversity and inclusion' and 'Safe Space reporting' sections have been moved to above the glossary.

c)   The 'Scope' section has been updated with the latest information for Microcredential learners.

d)   References to new policies relating to students in secure environments and those under legal licence restrictions, conditions or orders

e)   Some links have been updated.

f)   Some sections have been made clearer.

g)   Some glossary entries have been added or updated.

Policies superseded by this document

This document replaces the previous version of the Student Computing Policy dated March 2023.

Version number: 3.0	Approved by: Delegate of Director, Academic Services.
Effective from: August 2024	Date for review: March 2025