Computing Guidance:
for Professional Development (PD) learners
2022/23

Contents

1. Your CPD learner account [OUCP Section 3] ......................................................... 2
   1.1 Your CPD learner account and password [OUCP 3.1] ................................. 2
   1.2 Keeping your account secure [OUCP 3.2] .............................................. 2

2. Protection of Open University computer systems [OUCP Section 6] .................... 3
   2.1 Precautions you must take [OUCP 6.1] .................................................. 3
   2.2 What you are expected to do [OUCP 6.2] ............................................. 3

3. Standards of behaviour [OUCP Section 7] .......................................................... 4
   3.1 Acceptable standards [OUCP 7.1] ............................................................. 4

4. Using your computer safely [OUCP Section 10] ................................................. 5


6. Failure to comply [OUCP Section 12] .................................................................. 6

Appendix 1: The Open University Online Communications Principles [OUCP Appendix 2]... 7

Principle 1  The benefits of 'Digital Professionalism' .................................................. 7
Principle 2  Developing our skills ............................................................................. 7
Principle 3  Communicating effectively ..................................................................... 7
Principle 4  Managing our online image ................................................................. 7
Principle 5  Freedom of speech and ideas ................................................................. 7
Principle 6  Dignity and respect .............................................................................. 8
Principle 7  Criticising others and accepting criticism ............................................. 8
Principle 8  Confidentiality, privacy and copyright .................................................. 8
Principle 9  Responsibility and consequences ......................................................... 8
Principle 10 Moderation and control ...................................................................... 8

Version number: 1.0
Effective from: March 2022
Date for review: March 2023

The Open University is incorporated by Royal Charter (RC 000391), an exempt charity in England & Wales and a charity registered in Scotland (SC 038302). The Open University is authorised and regulated by the Financial Conduct Authority in relation to its secondary activity of credit broking.
The following guidance for your study of a Corporate and Professional Development (CPD) Course aligns with The Open University Computing Policy (as of June 2021). Related sections of this policy are noted in brackets. This guidance will be updated alongside any updates to The Open University Computing Policy.

For any questions regarding the content of this policy, please contact the CPD Support team.

<table>
<thead>
<tr>
<th>1. Your CPD learner account [OUCP Section 3]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.1 Your CPD learner account and password [OUCP 3.1]</strong></td>
</tr>
<tr>
<td>1.1.1 Our computing resources are provided for educational, training and research purposes. You must not use them for any business or significant personal purposes.</td>
</tr>
<tr>
<td>1.1.2 Your password must be in line with accepted good practice.</td>
</tr>
<tr>
<td><strong>1.2 Keeping your account secure [OUCP 3.2]</strong></td>
</tr>
<tr>
<td>1.2.1 It is your responsibility to keep your account secure and confidential. You are responsible for all activities carried out under your username. You must not give your password to anyone else or store it on another computer system. While you are logged into our system, you should not leave that computer unattended unless you can be sure that nobody else can use it while you are away, for example, you have a password-protected screen saver or you can lock the door behind you. To turn on the screensaver, press the Windows Key + L, or Ctrl+Alt+Del.</td>
</tr>
<tr>
<td>1.2.2 If you think the safety of your CPD learner account has been compromised, for example if somebody else knows your password, you must notify the CPD Support team. If you do not keep your account secure, you will be liable for any transactions relating to your registration and study, even if your password is used by someone else fraudulently or without your permission.</td>
</tr>
</tbody>
</table>
2. Protection of Open University computer systems

[OUCP Section 6]

2.1 Precautions you must take [OUCP 6.1]

2.1.1 The integrity of our computer systems is jeopardised if you do not take enough precautions against malicious software (for example, computer virus programs). You must not jeopardise the integrity, performance or reliability of computers, networks, software and other stored information that belong to us. ‘Software’ includes programs, routines, procedures and their associated documentation that can be used on a computer system, including personal computers and workstations.

2.2 What you are expected to do [OUCP 6.2]

2.2.1 You are expected to have and keep up to date virus protection software and take all reasonable steps to avoid distributing virus or malware to learners and other Open University computer users.

2.2.2 The Open University understands that individuals cannot control or prevent some unsolicited email; however, learners and other users must not send junk or phishing email or encourage others to do so. Your email software may have a ‘report junk’ function to enable you to report or block junk email sent to you.

2.2.3 You should be aware that email attachments may carry viruses, so if you are in any doubt, you must not open the email.

2.2.4 You should not download any software or files without up-to-date virus protection measures.

2.2.5 You should not visit hacking sites or download hacking or evidence eliminating software.

2.2.6 You should not intentionally visit, download or share in Open University systems, material from internet sites that are likely to contain obscene, racist, hateful or other objectionable materials.
2.2.7 You should not attempt to hack into other Open University computer users’ accounts or Open University systems by using password recovery, cracking, security analysis or any other security software.

2.2.8 You should not intentionally interfere with the normal operation of Open University and other student systems, including the propagation of computer viruses.

2.2.9 You should not cause sustained high-volume network traffic to The Open University that substantially hinders others in their use of the network, for example by sending emails to large numbers of addresses.

2.2.10 The University may automatically block or quarantine any email or post to an Open University website or forum identified as a potential threat to the organisation.

### 3. Standards of behaviour [OUCP Section 7]

#### 3.1 Acceptable standards [OUCP 7.1]

3.1.1 Acceptable standards of behaviour apply to computer-based information technology just as they would apply to other forms of communication:

a) Software or information we have provided may only be used for educational purposes unless agreed otherwise.

b) You must not send offensive, obscene or abusive information.

c) You must not present your own opinions or any facts or other information from your own sources as if they are those of The Open University or made on its behalf.

d) Any software, printed data or other information provided by the University must not be copied or used without prior permission from the University, software or information provider.

e) You must not break any copyright in documentation or software (or both). The Copyright, Designs and Patents Act 1998 gives copyright owners the right to bring civil proceedings if anyone breaks a copyright, and makes it a criminal offence to break certain copyrights. Specific legislation relating to computer programs can be found on the legislation.gov.uk website.
f) You must not use any Open University computing or network resources to use or publish material that is obscene, libellous or defamatory, or breaks our code of practice concerning harassment. You are personally responsible for your own activity on any Open University communications channel.

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

h) You must not do anything that damages our reputation, for example make threats against another student or a member of staff, share confidential information about the university, its students or staff, or make libellous statements about The Open University on social media sites.

3.2 Blocking content [OUCP 7.2]

3.1.2 The Open University may use software tools to block sites that are obscene, hateful or have other objectionable materials or may affect the University’s operations.

4. Using your computer safely [OUCP Section 10]

You should take care of your own health and safety when you are working on a computer.

5. Monitoring [OUCP Section 11]

5.1 In exceptional circumstances, we may have to use records of your contact with us and about your study to carry out our work or meet our legal obligations. The Executive Education (Corporate and Professional Development) Privacy Notice describes how we will manage these records.

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

5.3 The Open University has a statutory duty to have regard to the need to prevent people being drawn into terrorism. If the use of Open University computer equipment, information 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.
6. Failure to comply [OUCP Section 12]

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

6.2 Failure to comply with some aspects, may mean your learning experience is negatively impacted. For more serious breaches of the policy, for example around security and standards of behaviour, action may be taken under the [Code of Practice for Student Discipline](#). It may also be the case that your conduct and/or action(s) may be unlawful. The Open University reserves the right to inform the appropriate authorities in such cases.
Appendix 1: The Open University Online
Communications Principles [OUCP Appendix 2]

These principles describe the way in which Open University staff and students should work together online to support learning, research, administration and participation in all aspects of the University community.

Principle 1  The benefits of ‘Digital Professionalism’

Good online communication skills cannot be assumed, but they can be learned and are essential for effective engagement in learning and work. The development of ‘digital professionalism’ and skills in online communication has positive benefits for staff, for students and for employability.

Principle 2  Developing our skills

We will support each other to learn, develop and enhance our online communications skills, through advice, guidance, learning resources and working together.

Principle 3  Communicating effectively

We will support and encourage clear and effective communication in online situations and the use of language, style and tone which is relevant and appropriate to the circumstances and the purpose of the communication.

Principle 4  Managing our online image

We will ensure that we are all aware of the importance of managing our digital footprint and support each other to raise awareness of the benefits of creating a positive online image and how to achieve it. We will be mindful of maintaining our own confidentiality and personal security.

Principle 5  Freedom of speech and ideas

We will promote the open exchange of ideas and uphold the fundamental principle of freedom of speech and thought. We acknowledge that people have the right, within the law, to hold and to express ideas that others may find challenging. We will not allow views to be presented in a way that is hostile or degrading to others.
Principle 6  Dignity and respect
We will treat each other with dignity and respect, even where we disagree with each other, and be sensitive to the impact our conduct may have on other students and staff. We recognise that good manners aid effective communication. We aim to be welcoming and inclusive and do not provide a platform for threats, personal abuse, derogatory comments, unreasonable behaviour that causes offence, discrimination, victimisation, bullying or harassment.

Principle 7  Criticising others and accepting criticism
We should be prepared to accept legitimate criticism, provided it is within the law, based on accurate facts, measured and in an appropriate forum. It is rarely appropriate for named individuals to be criticised in public or anywhere that they have no right or opportunity to reply.

Principle 8  Confidentiality, privacy and copyright
We will respect each other’s confidentiality and privacy and we will not share personal details or distribute ideas, words and images that belong to others without their express or implied permission and without acknowledgement. We will not tolerate plagiarism or activities which encourage or enable it.

Principle 9  Responsibility and consequences
We will accept responsibility for our own actions and encourage others to do so. We should be aware that poor communication skills and unacceptable behaviour may have a negative impact on others.

Principle 10  Moderation and control
Moderators and other controllers of online communication spaces, whether they are staff or students, have a responsibility to uphold these principles. The aim of moderation or control is to provide an environment within which meaningful, relevant and effective communication can take place. Moderators’ decisions should be open, transparent and consistent with any relevant guidelines, which should be available to all participants. Moderators have the right to expect reasonable decisions to be respected but must be prepared for some decisions to be challenged, through appropriate channels.