# Computing Guidance: for Professional Development (PD) learners

2023/24

## 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 Keeping your computer and our systems safe [OUCP 6.1] ............................................................................................ 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  
5. Monitoring [OUCP Section 8] ........................................................................................................................................... 5  
6. Failure to comply [OUCP Section 9] ............................................................................................................................... 6
The following guidance for your study of a Corporate and Professional Development (CPD) Course aligns with The Open University Computing Policy (as of March 2023). 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.

1. **Your CPD learner account** [*OUCP Section 3*]

1.1 **Your CPD learner account and password** [*OUCP 3.1*]

1.1.1 You will be provided with a secure CPD computing account when you register. This will give you access to the CPD computing services you need for your studies. You should not use your account for any business or personal purposes.

1.1.2 Your password must be in line with accepted good practice.

1.1.3 You must not share the contact details of any CPD student or staff member, including computer username and email address, without their express permission.

1.2 **Keeping your account secure** [*OUCP 3.2*]

1.2.1 You should always keep your account secure and confidential; your account details should not be accessible to anyone else.

1.2.2 If you think the security of your CPD Learner account has been compromised, for example if somebody else knows your password, you must notify the CPD Support team 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.
2. Protection of Open University computer systems

[OUCP Section 6]

2.1 Keeping your computer and our systems safe [OUCP 6.1]

2.1.1 Working online may expose both you and our computer systems to external threats, 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 should 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. If in doubt, do not open suspicious email.

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 other objectionable materials, nor download or share such material via Open University systems.

e) Do not publish any content that might contain obscene, racist, hateful or other objectional material 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 network 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) If you think you may have compromised our network, you must contact the CPD Support team immediately. We may investigate any breach or potential breach by accessing all relevant records and other evidence.
3. Standards of behaviour [OUCP Section 7]

3.1 Acceptable standards [OUCP 7.1]

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

a) That you should only use our computing services for the purpose of your study with us unless we have agreed otherwise.

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 The Open University’s reputation.

d) You should 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.

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. You should not share online any questions relating to assessment nor any completed assessments. For further details, please see section 3.3, Enabling Plagiarism, in our Academic Conduct Policy.

If you realise you have unintentionally enacted any of (a) to (e) above, you should determine if you can undo what you have done. Otherwise, you should contact the CPD Support team and explain the situation immediately.

f) 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).

g) 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.

h) 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.

i) Users accessing our computing services from outside the UK must ensure that they abide by all local laws. 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.

j) 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

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 8]

5.1 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 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’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.

5.3 As an institution of higher education, we have a statutory duty to prevent people being drawn into terrorism. If the use of Open University 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.
6. Failure to comply [OUCP Section 9]

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 If you fail to manage your Open University computing account as stated in Section 1.1 above, it may adversely affect your learning experience. For more serious breaches of the policy, such as those related to security (section 2) or standards of behaviour (section 3), 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, in which case, we may inform the appropriate authorities.