

POLICIES & PROCEDURES

TITLE	Learner IT & Use of Resources Policy
AUTHOR	REDBRIDGE INSTITUTE
RESPONSIBLE OFFICER	Facilities Manager
APPROVED BY GOVERNING BODY OR INTERNAL PROCEDURE APPROVED BY SMT	GOVERNING BODY
DATE OF DRAFT SUBMISSION TO GOVERNING BODY	December 2016
DATE OF APPROVAL	December 2016
REVIEW DATE	December 2019

Equality Impact Assessment

Completed by Redbridge Institute		Not applicable – no significant changes	√
Completed by London Borough of Redbridge		Outstanding	

Introduction

Redbridge Institute provides IT resources for learners and other users to support and enhance their learning or to allow work to be carried out for or on behalf of the Institute. As well as providing IT resources within the classroom, learners may use the facilities in the Learning Resource Centre and the internet café.

Learners and other users of Redbridge Institute's IT resources must meet the requirements set out in this document. These requirements are designed to protect Redbridge Institute's IT infrastructure and data and define Redbridge Institute's views on what constitutes acceptable use of the IT resources it provides. These requirements enable Redbridge Institute to comply with procedural and legal frameworks and requirements.

All computer or network users should read and follow these requirements and guidelines, make themselves aware of the potential liabilities involved in using computers, e-mail and the internet and understand Redbridge Institute's expectations of how its IT resources should be used.

Requirements for using Redbridge Institute's IT resources

1. Learners must not use Redbridge Institute's IT systems to obtain, manipulate or distribute material which may be considered offensive or inappropriate in any way. Redbridge Institute will make the final decision on whether material is offensive or inappropriate but this will include material which is clearly pornographic, homophobic, sexist, racist or abusive.
2. Learners should report any issues of cyber bullying and inappropriate or harassing online communications to their tutor or a member of the Senior Leadership Team. The Stay Safe On-Line guide is available on the website.
3. Users must not change computer settings or install software on Redbridge Institute's computers. IT staff are the only people authorised to install software, perform maintenance or move IT equipment within Redbridge Institute. If you see anyone tampering or moving any computer equipment please inform a Redbridge Institute employee immediately.
4. Users must not run applications which are not already installed on Redbridge Institute computers.
5. Users must not copy Redbridge Institute software or use logos or other Institute images without authorisation.
6. Learners must check that memory sticks are free of viruses and inappropriate or illegal material before using them at Redbridge Institute. Learners who knowingly bring viruses or other malware into Redbridge Institute may be disciplined.
7. Apart from USB memory sticks or similar storage devices, no IT equipment or devices should be physically connected to the Redbridge Institute teaching network. This includes cameras, tablets, laptops, portable hard drives, phones etc. Doing so may result in disciplinary action.
8. Learners may use their own laptop, phone or other portable device to connect to the student wireless network provided by Redbridge Institute.

9. Redbridge Institute's wireless networks may only be used by learners or guests of Redbridge Institute.
10. There is no private storage area for learners' or guests' files or data. Any information on Redbridge Institute's teaching network may be read, copied or modified by other learners. Users must not store personal data on Redbridge Institute computers or networks and are advised that all learner computers in teaching rooms and the Learning Resource Centre are wiped clean every evening.
11. Internet content is filtered to prevent staff, learners and guests from accessing or viewing inappropriate material and harmful files using Palo Alto Firewall with additional filtering through the internet supplier Janet UK. Learners must inform a member of Redbridge Institute's staff immediately if they find an inappropriate site is accessible. Learners should be aware that the Police may be called if criminal activity is suspected. Learners also have a duty to report to the safeguarding team on safeguarding@redbridge-iae.ac.uk other users who they suspect may be engaged in research or activities which could relate to criminal activities or to the support of terrorism or radicalisation.
12. Internet access is monitored. Inappropriate usage may lead to disciplinary action.
13. Learners must not download or use copyright protected material, data or information unless they have the permission of its owner or owners or usage falls within current permitted rights.
14. Copyrighted software must never be downloaded. The use of peer-to-peer services for downloading such material is strictly prohibited.
15. Learners who have been given access to Redbridge Institute's online information systems, for example, moodle or bksb:
 - a. are responsible for all activity made using their online account
 - b. must not give their password to anyone else.
 - c. must inform Redbridge Institute's IT Services if they believe their account is being used by someone else
 - d. must not share their login details
 - e. should not attempt to log on as someone else or use a computer while somebody else is logged in.
 - f. must ensure they log out of all services when they have finished using them.
16. Redbridge Institute is not responsible for files, data or information stored on external services, for example Microsoft's SkyDrive, Google's Drive, Dropbox or similar services.
17. Learners should check that IT workstations, chairs and other equipment are in the right position for their own use so the computers are comfortable and easy to use. Redbridge Institute's IT and Facilities teams can advise learners on how to adjust a workstation. Redbridge Institute's Learning Support Coordinator can help with equipment or adaptations that may be needed by learners with additional needs.
18. Learners are expected to print responsibly and only when necessary. On-screen print preview and proofing tools can be used to check documents before printing. Learners

will be charged for printing generated from the Learning Resource room and may be asked to pay for printing within the classroom.

Compliance

Users failing to comply with the requirements of this policy may be subject to action under the learner disciplinary policy.