LANCASTER TRAINING SERVICES LTD

Regulations for the use of computing facilities

1 Scope

1.1 Users

These regulations apply to everyone using LTS's computing facilities. In particular they apply to staff and learners at LTS, and to people outside the training centre who have been given permission to use the Training Provider's facilities.

1.2 Permission to use the LTS's computing facilities

Users should be aware that the Training Provider retains the right to monitor messages and materials sent over its network to check that the user is not in breach of any regulations outlined in this document.

1.3 Facilities

The computing facilities covered by these regulations include all computers located in the training centre, including multi-user hosts, workstations and personal computers, together with the software and data stored on them. The regulations also cover all computing carried out on a computer connected to the training provider's network, whether or not this involves the use of Training Provider-based or Training Provider-owned computer.

2 Relevant legislation

Users must comply with all UK legislation relating to the use of information, computers and networks.

2.1 Computer misuse

Users must not:

(a) access (or display any information which permits another to access) computer material without authorisation for perpetration of any criminal offence;

(b) alter (or display any information which permits another to alter) data, programs, files, electronic mail or any other computer material belonging to another user without the other user's permission;

(c) use (or display any information which permits another to use) a computer to access any program or information which they are not authorised to access/use.

2.2 Copyright and rights in software

The Training Provider expressly forbids the illegal copying of software by staff or learners. All users must respect rights in proprietary software and other on-line information. Users may not copy proprietary data from any systems without permission, nor install proprietary software on systems not covered by an appropriate licence.

The Training Provider may carry out audits from time to time to ensure all software is legal.

Many software packages in the training centre are licensed only for educational use, and must not be used for commercial purposes unless a full licence is obtained.

Disciplinary action will be taken against staff or learners who knowingly make, acquire or use unauthorised copies of computer software.

Users may not upload or download information through the Training Provider's computing facilities which is not authorised by the copyright owner or permitted by law. Users must not make, transmit or store electronic copies of copyright material on the Training Provider's computing facilities without the permission of the owner. A serious breach of copyright could result in disciplinary action.

2.3 Data Protection

Any work involving processing, storing or recording personal data (i.e. information on an identifiable individual) is subject to the Data Protection act 2018 in particular the General Data Protection Regulation (EU) 2016/679 (GDPR). It is the user's responsibility to ensure that personal data is collected in accordance with the Act. Personal data must be fairly obtained, securely stored and access only given to those who need it.

Users must:

(a) in cases of doubt, contact the Training Provider's Data Protection Officer before conducting an activity which involves the collection, storage or display of personal data, to find out whether the proposed use of personal data complies with the Training Provider's notification;

(b) ensure that all records containing personal data are accurate and up-to-date. You should not keep personal data records for longer than is necessary;
(c) carefully review any disclosures of personal data, both within and, particularly, outside the EEA;
(d) ensure that all information stored on a computer is professionally removed when the computer is passed to another user, sold or otherwise disposed of.
(e) ensure that personal data is not taken home or stored on a home computer.
Failure to comply with the terms of the Data Protection Act may result in both criminal charges and civil actions for compensation. A serious breach of the Act could constitute a serious disciplinary offence and will result in internal disciplinary action.

2.4 Offensive or defamatory material

All information that is made available on-line to other people, either by electronic mail or in publicly accessible file space (for example on the World Wide Web) must not be discriminatory, pornographic, homophobic, excessively violent, obscene, libellous, blasphemous, seditious, incite racial hatred, or in any way break any law pertaining to published material. Users must not access, store, display, receive, download or transmit offensive, extremist (Prevent Duty) or obscene material.
In addition, users must not publish any information on-line which will cause offence or needless anxiety to people who might normally be expected to read it, or make any defamatory statement. A defamatory statement could be contained in articles, letters, emails and visual images. Users must not use threatening, abusive or otherwise objectionable language in either public or private messages.
The Training Provider will regard the publication or possession of offensive or obscene material as a serious disciplinary matter and, with regard to obscene materials, will not hesitate to inform the police. In the unlikely event that there is a genuine academic need for accessing offensive or defamatory material, the Training Provider must be made aware of this and prior permission must be granted from the Training Manager.

2.5 Discrimination

Users must not use the Training Provider's computing facilities to place, disseminate or receive materials which discriminate or encourage discrimination on the grounds of gender, sexual orientation, disability, race or ethnic origin.

2.6 Official Secrets Acts 1911 - 1989

The Official Secrets Acts 1911-1989 establish severe criminal penalties for any person who discloses any material which relates to security, intelligence, defence or international relations and which has come into that person's possession through an authorised or unauthorised disclosure by a Crown Servant or Government contractor.
Users must ensure that any such material is securely stored and avoid displaying it on the Training Provider's computing facilities.

3 Use of Training Provider’s computing facilities

3.1 Access

Users must not provide access to any of the Training Provider's computing facilities to those not rightfully due such access. Any activity carried out by a user for any fee or other consideration is in contravention of these regulations unless prior approval has been obtained from the Training Manager or, the head of department. The Training Provider's computing facilities must not be used for placing or distributing advertisements relating to any course of business other than those promoting the Training Provider's teaching and research activities or its own trading operations.

3.2 Identification

Users may not use a personal identifier or passwords allocated to another user, nor pass their own personal identifier or password to another person. Users may not pass themselves off as another person when sending electronic mail or making information available on-line in any other way. No device attached to the Training Provider's network may be configured with any addresses other than those issued to it or authorised for it by appropriate staff in the Training Centre.

3.3 Compliance with Policies, Codes and Regulations

Users must comply with the relevant Acceptable Use Policies associated with all computer networks of which use is made. If computing facilities at another site are employed, users must comply with the regulations and codes governing that site.

3.4 Responsible use of the Training Provider's computing facilities

Computing facilities are provided for use by staff in the course of their employment and by learners in the course of their education. While other incidental and occasional use may be permitted such use must not interfere with the employee's work or the learner's study. Any abuse of such permission will be treated as a contravention of these regulations.

The following will also be treated as contravening these regulations:

(a) any action that would impair the function or security of the Training Provider's computer network;
(b) any action that denies another network user access to network services;
(c) connecting any device to the Training Provider's network without first registering the device with the appropriate staff member;
(d) attempts to penetrate security and/or privacy of other users' files;
(e) any use of the Training Provider's computing facilities that brings the Training Provider into disrepute;
(f) making, storing or transferring unlicensed copies of any copyright or trademark work including computer programs;
(g) setting up web servers, or placing web pages on any of the Training Provider's computing equipment, other than that provided for the purpose by the Training Provider;
(h) sending bulk e-mail material unrelated to the legitimate educational business of the Training Provider, including the transmission of bulk e-mail advertising (spamming);
(i) sending unsolicited e-mail messages requesting other users, at the Training Centre or elsewhere, to continue forwarding such e-mail messages to others, where those e-mail messages have no educational or informational purpose (chain e-mails);
(j) sending e-mails which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing);
(k) sending or receiving material which is illegal under UK law, which may give rise to legal action against the user and/or the Training Provider, or which contravenes any of the Training Provider's regulations or guidelines.

Many computers in the Training Centre provide access to computer networks that enable users not only to connect to computers at other educational establishments, but also to connect to computers at many sites not related to the education sector. The ability to connect to a computer does not automatically give users the authority to use it. If the system displays a message that explicitly states that users do not need to be authorised to use it, they may use the system. If there is no explicit message, users should not attempt to use the system. System administrators are obliged to inform the Training Manager of any detected or suspected misuse of the systems for which they are responsible.

4 Supervision

The Trainer/Tutor of the group/individual will oversee the safe use of technology, including internet and take immediate action if they are concerned. It is vital that all IT activities are supervised and monitored **at all times.** Safeguarding/Prevent issues will be reported to the DSL. Learners must NOT be given access to the Centre's Wi-Fi.

5 Penalties

5.1 Withdrawal of facilities

If a user is in breach of any of these regulations, the Training Manager may withdraw or restrict his or her use of computing facilities, following consultation where appropriate with the user's head of department.

5.2 Disciplinary action

Any breach of the regulations may be reported to the Training Manager to be dealt with under the Training Provider's disciplinary procedures. The Training Manager may request that a user be charged for extra work or expenses that have arisen as the result of computer misuse.

5.3 Breaches of the law

Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach will be reported to the relevant authorities within that jurisdiction.

Richard W Little – Chairman

Document Control	
Issued	24/8/16
Version	2
Reviewed	Aug 18
Next Review	Oct 19
Owner	M Horabin
Title	Training Manager