Learning
Development
Training

Education | Inspires | Change

IT Acceptable Use Policy Guidance

Version Number	V1
Date Approved	January 2020
Last Review Date	18/8/20
Scheduled Review Date	August 2021

This guidance expands on the principles set out in the policy. It gives many examples of specific situations and is intended to help you relate your everyday use of the IT facilities to the do's and don'ts in the policy.

Where a list of examples is given, these are just some of the most common instances, and the list is not intended to be exhaustive.

Where the terms similar to Authority, Authorised, Approved or Approval appear, they refer to authority or approval originating from the person or body identified in section 3, Authority, or anyone with authority delegated to them by that person or body.

1. Scope

1.1 Users

This policy applies to anyone using LDT IT facilities. This means more than students and staff. It could include, for example:

- External partners, contractors and agents based onsite and using LDT network, or offsite and accessing LDT's systems;
- Staff, students or associates of LDT using LDT's computers, servers or network;
- Visitors using LDT's Wi-Fi;
- Students and staff from other LDT s logging on to Wi-Fi.

1.2 IT facilities

The term IT facilities include:

- IT hardware that LDT provides, such as PCs, laptops, tablets, smart phones and printers;
- Software that LDT provides, such as operating systems, office application software, web browsers etc. It also includes software that LDT has arranged for you to have access to, for example, special deals for students on commercial application packages;
- Data that LDT provides, or arranges access to. This might include online journals, data sets or citation databases;
- Access to the network provided or arranged by LDT. This would cover, for example, network connections in halls of residence, on campus Wi-Fi, connectivity to the internet from LDT PCs;

- Online services arranged by LDT, such as Office 365 and Google Apps, any online resources;
- IT credentials, such as the use of your LTU login, or any other token (email address, smartcard, dongle) issued by LTU/LDT to identify yourself when using IT facilities. For example, you may be able to use drop in facilities at other LDT sites using your usual username and password through the LDT system. While doing so, you are subject to this policy, as well as the regulations at LDT site you are visiting.

2. Governance

It is helpful to remember that using IT has consequences in the physical world.

Your use of IT is governed by IT specific laws and regulations (such as this policy), but it is also subject to general laws and regulations such as LDT's general policies.

2.1 Domestic law

Your behaviour is subject to all relevant laws of the United Kingdom, even those that are not apparently related to IT such as the laws on fraud, terrorism, theft and harassment.

- Freedom of Information (Scotland) Act 2002 www.legislation.gov.uk/asp/2002/13/contents
- Equality Act 2010 www.legislation.gov.uk/ukpga/2010/15/contents
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) www.legislation.gov.uk/uksi/2003/2426/contents/made
- Defamation Act 1996 www.legislation.gov.uk/ukpga/1996/31/contentsand Defamation Act 2013 www.legislation.gov.uk/ukpga/2013/26/contents
- Counter Terrorism and Security Act 2015 www.legislation.gov.uk/ukpga/2015/6/contents

For example, you may not:

- Create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- Create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety;
- Create or transmit material with the intent to defraud;
- Create or transmit defamatory material;
- Create or transmit material such that this infringes the copyright of another person or organisation; e.g. No uploading/downloading/sharing of illegal, pirated or unlicensed content (images, films, software, music).
- Create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe;
- Deliberately (and without authorisation) access networked facilities or services.

2.2 Foreign law

If you are using services that are hosted in a different part of the world, you may also be subject to their laws. It can be difficult to know where any particular service is hosted from, and what the applicable laws are in that locality.

In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

2.3 Additional applicable policies

The details of acceptable usage in specific areas may be found in the following list of LDT Policies:

- IT Asset Management Policy
- IT Remote Working Policy

2.3 Third party regulations

If you use LDT IT facilities to access third party services or resources, you are bound by the regulations associated with that service or resource. (The association can be through something as simple as using your LDT/LTU username and password).

Very often, these regulations will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it.

There will be other instances where LDT has provided you with a piece of software or a resource.

- License agreements

Users shall only use software and other resources in compliance with all applicable licenses, terms and conditions.

3. Authority

Authority to use LDT's IT facilities is granted by a variety of means:

- The issue of a username and password or other IT credentials
- The explicit granting of access rights to a specific system or resource
- The provision of a facility in an obviously open access setting, such as an LDT website; a wok station in a public area; or an open Wi-Fi network on LDT premises.

If you have any doubt whether or not you have the authority to use an IT facility you should seek further advice from **darren@ldtraining.org.uk**

Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act.

4. Intended use

Elements of LDT IT facilities, and the Janet network that connects LDT s together and to the internet, are funded by the tax paying public. They have a right to know that the facilities are being used for the purposes for which they are intended.

4.1 Use for purposes in furtherance of LDT's mission

The IT facilities are provided for use in furtherance of LDT's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of LDT, or the administration necessary to support all of the above.

4.2 Personal use

Students may currently use the IT facilities for personal use provided that it does not breach the policy, and that it does not prevent or interfere with other people using the facilities for valid purposes (for example, using a PC to update your Facebook page when others are waiting to complete their assignments).

However, this is a concession and can be withdrawn at any time.

Employees using the IT facilities for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity. In general, the use of any IT facilities should be in a manner that is consistent with your role.

4.3 Commercial use and personal gain

Use of IT facilities for non-LDT commercial purposes, or for personal gain, such as running a club or society, requires the explicit approval of the Director and/or the Senior Management Team. The provider of the service may require a fee or a share of the income for this type of use.

Even with such approval, the use of licenses for anything other than teaching, studying or research, administration or management purposes is prohibited, and you must ensure that licenses allowing commercial use are in place.

5. Identity

Many of the IT services provided require you to identify yourself so that the service knows that you are entitled to use it.

This is most commonly done by providing you with a username and password, but other forms of IT credentials may be used, such as an email address, a smart card or some other form of security device.

5.1 Protect identity

You must take all reasonable precautions to safeguard any IT credentials issued to you.

You must change passwords when first issued and at regular intervals as instructed. Do not use obvious passwords, and do not record them where there is any likelihood of someone else finding them. Do not use the same password as you do for personal (i.e. non-LDT al) accounts. Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.

If you think someone else has found out what your password is, change it immediately and report the matter to IT darren@ldtraining.org.uk

Do not use your username and password to log in to websites or services you do not recognise, and do not log in to websites that are not showing the padlock symbol.

Do not leave logged in computers unattended, and log out properly when you are finished.

5.2 Impersonation

Never use someone else's IT credentials, or attempt to disguise or hide your real identity when using LDT's IT facilities.

However, it is acceptable not to reveal your identity if the system or service clearly allows anonymous use (such as a public facing website).

5.3 Attempt to compromise others' identities

You must not attempt to usurp, borrow, corrupt or destroy someone else's IT credentials.

5.4 Changing your password

If you forget your password, you can go to one of the on-campus service desks and request it be reset in person. You will need to prove your identity to do this.

6. Infrastructure

The IT infrastructure is all the underlying stuff that makes IT function. It includes servers, the network, PCs, printers, operating systems, databases and a whole host of other hardware and software that has to be set up correctly to ensure the reliable, efficient and secure delivery of IT services.

You must not do anything to jeopardise the infrastructure. Any device that is found to be disrupting or degrading the operation of the infrastructure intentionally or otherwise is subject to disconnection.

6.1 Physical damage or risk of damage and loss

Do not damage, or do anything to risk physically damaging the infrastructure, such as being careless with food or drink at a PC, or playing football in a drop in facility.

Do protect LDT IT equipment that is on loan to you or otherwise being used outside LDT from improper use. i.e. Friends, relatives etc. must not be given use of this equipment.

You must immediately report any lost or stolen equipment to the IT Department darren@ldtraining.org.uk

6.2 Reconfiguration

Do not attempt to change the setup of the infrastructure without authorisation, such as changing the network point that a PC is plugged in to, connecting devices to the network (except of course for Wi-Fi or Ethernet networks specifically provided for this purpose) or altering the configuration of LDT's PCs. Unless you have been authorised, you must not add software to or remove software from PCs.

Do not move equipment without authority.

6.3 Network extension

You must not extend the wired or Wi-Fi network without authorisation. Such activities, which may involve the use of routers, repeaters, hubs or Wi-Fi access points, can disrupt the network and are likely to be in breach of LDT Security Policy.

6.4 Setting up servers

You must not set up any hardware or software that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, IRC servers or websites without authority.

6.5 Introducing malware

You must take all reasonable steps to avoid introducing malware to the infrastructure. LDT may refuse or disconnect devices that are not adequately protected from malware infection.

The term malware covers many things such as viruses, worms and Trojans, but basically any software used to disrupt computer operation or subvert security. It is usually spread by visiting websites of a dubious nature, downloading files from untrusted sources, opening email attachments from people you do not know or inserting media that have been created on compromised computers.

If you avoid these types of behaviour, keep your antivirus software up to date and switched on, and run scans of your computer on a regular basis, you should not fall foul of this problem.

6.6 Subverting security measures

LDT has taken measures to safeguard the security of its IT infrastructure, including things such as antivirus software, firewalls, spam filters, security permissions and so on.

You must not attempt to subvert or circumvent these measures in any way.

6.7 Using your own devices

Personal devices may be connected to LDT Wi-Fi network only. LDT expects that your device will have adequate malware protection and any software it contains be properly licensed. When you connect your device to LDT network you do so at your own risk. LDT accepts no responsibility for consequential damage, virus infection, corruption or loss.

Please be aware that LDT WiFi is ultimately a public funded network and LDT is obliged to track device usage to guard against any illegal activity.

7. Information

7.1 Personal, sensitive and confidential information

During the course of their work or studies, staff and students (particularly research students) may handle information that comes under the General Data Protection Regulations and the Data Protection Act 2018, or is sensitive or confidential in some other way. For the rest of this section, these will be grouped together as protected information.

Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. LDT has policies on Data Protection and Information Management and if your role is likely to involve handling protected information, you must make yourself familiar with, and abide by, these policies.

7.1.1 Transmission of protected information

When sending protected information electronically, you must use a method with appropriate security. Email and many other means of transmitting data are not inherently secure.

7.1.2 Removable media and mobile devices

Highly Confidential information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablets or smartphones) unless it is encrypted, and the key kept securely.

If protected information is sent using removable media, you must use a secure, tracked service so that you know it has arrived safely.

7.1.3 Remote working

If you access protected information from off campus, you must make sure you are using an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service. These are detailed in LDT's Remote Working Policy.

You must also be careful to avoid working in public locations where your screen can be seen.

7.1.4 Personal or public devices and cloud services

Even if you are using approved connection methods, devices that are not fully managed by LDT cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. You should not therefore use such devices to access, transmit or store protected information.

Staff must not store protected information on personal cloud services such as Dropbox. For more detailed guidance on the safe usage of third party storage systems, definitions of protected information please consult LDT's Information Security Policy.

7.2 Copyright information

Almost all published works are protected by copyright. If you are going to use material (images, text, music, films, software), the onus is on you to ensure that you use it within copyright law. This is a complex area, and training and guidance are available from LTU's Legal Services Department. The key point to remember is that the fact that you can see something on the web, download it or otherwise access it does not mean that you can do what you want with it.

All software on any equipment connected to an LDT network must be properly licensed and the terms of the license strictly observed.

7.3 Others' information

You must not attempt to access, delete, modify or disclose restricted information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you have approval.

Where information has been produced in the course of employment by LDT, and the person who created or manages it is unavailable, the responsible line manager may give permission for it to be retrieved for work purposes. In doing so, care must be taken not to retrieve any private information in the account, nor to compromise the security of the account concerned. See Privacy and Monitoring Policy.

You must report any unintended access to information. e.g. Notify the sender of any email you receive that is clearly intended for someone else. The same applies should you find you have inappropriate access to information or systems. E.g. you can access resources you shouldn't be able to, report these to the relevant resource controller.

Private information may only be accessed by someone other than the owner under very specific circumstances governed by LDT and/or legal processes. See Privacy and Monitoring Policy

7.4 Inappropriate material

LDT has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. LDT reserves the right to block or monitor access to such material.

LDT has procedures to approve and manage access to such material for valid research purposes. There is an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of policy or the law.

7.5 Publishing information

Publishing means the act of making information available to the general public, this includes through websites, social networks and news feeds. Whilst LDT generally encourages publication, there are some general guidelines you should adhere to:

7.5.1 Representing LDT

You must not make statements that purport to represent LDT without the approval of the Governing Board.

7.5.2 Publishing for others

You must not publish information on behalf of third parties using LDT 's IT facilities without the approval of the Governing Board.

8. Behaviour

The way you behave when using IT should be no different to how you would behave under other circumstances. Abusive, inconsiderate or discriminatory behaviour is unacceptable. Your use of facilities should be consistent with your role.

8.1 Conduct online and on social media

All use of IT facilities shall be lawful, honest and decent and shall have regard to the rights and sensitivities of other people.

You should not deliberately create, use or distribute materials that could bring LDT into disrepute.

LDT policies concerning staff and students also apply to the use of social media.

8.2 Spam

You must not send unsolicited bulk emails or chain emails.

8.3 Denying others access

If you, as a student, are using shared IT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them.

8.4 Disturbing others

When using shared spaces, remember that others have a right to work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area), do not obstruct passageways and be sensitive to what others around you might find offensive.

8.5 Excessive consumption of bandwidth/resources

Use resources wisely. Don’t consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. You should manage resources allocated to you effectively. E.g. don’t allow yourself to run out of file or email storage space. Doing so will hinder your ability to use IT services. Do not waste paper by printing more than is needed, or by printing single sided when double sided would do. Don’t waste electricity by leaving equipment needlessly switched on.

8.6 LDT monitoring

LDT monitors and logs the use of its IT facilities for the purposes of:

- Detecting, investigating or preventing misuse of the facilities or breaches of LDT policy;
- Monitoring the effective function of the facilities;
- Investigation of alleged misconduct;

For more information, please refer to LDT’s Privacy and Monitoring Policy

8.7 Unauthorised monitoring

You must not attempt to monitor the use of IT without the explicit permission of the Director, IT and Communications Services.

This would include:

- Monitoring of network traffic;
- Network and/or device discovery;
- Wi-Fi traffic capture;
- Installation of key logging or screen grabbing software that may affect users other than yourself;
- Attempting to access system logs or servers or network equipment.

Where IT is itself the subject of study or research, special arrangements will have been made, and you should contact your course leader/research supervisor for more information.

9. Infringement

9.1 Disciplinary process and sanctions

Breaches of this policy will be handled by LDT’s disciplinary processes.

This could have a bearing on your future studies or employment with LDT and beyond.

Sanctions may be imposed if the disciplinary process finds that you have indeed breached the policy, for example, imposition of restrictions on your use of IT facilities; removal of services; withdrawal of offending material; fines and recovery of any costs incurred by LDT as a result of the breach.

9.2 Reporting to other authorities

If LDT believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency

If LDT believes that a breach of a third party’s regulations has taken place, it may report the matter to that organisation.

9.3 Report infringements

If you become aware of an infringement of this policy, you must report the matter to the IT Department: darren@ldtraining.org.uk