



## **Acceptable Use Policy for Internet, Email and ICT**

*This policy incorporated LGEC's previous "Communications Policy"*

### **Introduction**

This acceptable use policy (AUP) describes the rights and responsibilities of anyone using LGEC's electronic resources, such as computers, the Internet, video cameras and so on. It explains the procedures that all staff and volunteers within LGEC are expected to follow and makes clear what is considered acceptable behaviour when using it. It also contains guidelines on using LGEC's resources effectively including procedures on data management and security.

### **Background**

There are many common benefits that LGEC have benefited from with the improvement of ICT resources. The speed of communication is probably the biggest benefit of e-mail, with the ability to contact an individual or specified group of people at the same time if required. This generally improves internal and external communications of LGEC, although it does not follow that a reply will be received as quickly.

Improved ICT resources have also helped improved efficient and flexible working arrangements at LGEC, allowing easier working arrangements when staff need to work from home. The internet has also provided LGEC with wider opportunities for research via the Internet, improving the efficiency of recruitment, allows for the submission of documents and reports via email, and allows for the provision of an e-commerce "shop-window" for the organisation via our website.

### **Challenges of electronic communications**

However, electronic communications also pose a number of possible problems, which may include:

- E-mail is not the informal and transient form of communication that many people think it is, even 'deleting' a message does not mean it is unrecoverable.
- Intensive use of e-mail, and unnecessarily wide broadcasting, can lead to 'information overload' and stress as staff members try to keep up with the number of e-mails received.
- The ease and speed of e-mail can lead to inadequate thought going into a message, and the possibility of the words or tone being misinterpreted by the recipient.
- Sites visited via the Internet are traceable.
- There are a number of laws that cover electronic communications including copyright and licensing restrictions (see section 6).
- It is essential that LGEC considers the impact these might have, the position of workers and the legal liabilities that may be incurred.

### **Policy content**

The content of this AUP is made up of the following:

1. Personal usage
2. Email guidelines
3. Good housekeeping practices and password security
4. Inappropriate email messages
5. Accessing inappropriate material
6. Copyright and licensing restrictions
7. What might happen if a breach of this policy occurs.
8. LGEC's ICT network guidelines

-

## **1. Personal usage**

Access to LGEC's ICT resources including the internet during working time should be limited to matters relating to your employment. Reasonable personal use of the internet by staff members outside of work time is permitted, providing these do not interfere with individual work responsibilities.

LGEC's ICT resources including the internet will not be used under any circumstances and at any time to deliberately access offensive, obscene or indecent material from the internet, such as pornography, racist or sexist material, violent images and incitement to criminal behaviour. LGEC's ICT resources will also not be used to access inappropriate messages, for instance any which might cause offence or harassment on grounds of sex, race, disability, age, religion.

The following circumstances also need to be considered by staff members using LGEC's ICT resources outside of work time:

### **Downloading large files**

While LGEC do not have any limitation on the amount of data downloaded via our Internet Service Provider, the download of large files such as music or video files do cause valuable hard drive space to be used unnecessarily. Any such files considered as "reasonable use" should therefore be saved directly onto a staff member's own memory stick. Files should also be downloaded from "trusted" sites only.

### **Messaging/chat**

Staff members should be aware that use of chat programmes like MSN, social networking sites including You Tube should be aware that malicious code can be launched on websites such as these, and can unintentionally infect an entire network if an employee accesses the website on a computer which is not protected against such attacks. LGECs ICT network does run anti-spy ware and virus programmes, but accessing such sites should be done with caution.

## **2. Email guidelines**

As well as the many benefits of e-mail, it is essential that all staff members realise the following potential pitfalls with e-mail:

- It is not an informal communication tool, but has the same authority as any other communication to and from the organisation.
- External e-mails should have disclaimers attached.
- It should be regarded as published information.
- E-mails are not confidential, and can be read by anyone given sufficient levels of expertise

### **Additionally, staff members should be aware that:**

- Legally binding contracts may be inadvertently created.
- Defamation of colleagues or other parties (deliberate or otherwise) may occur.
- Abrupt, inappropriate and unthinking use of language can lead to a bullying tone and possible offence to others, even harassment. For example, capitals are often interpreted as shouting.
- Consider whether a phone call may be a better way of discussing a complex or confidential matter.

### **LGEC considers the following as unacceptable use of email:**

- Use of LGEC resources to send chain letters
- Forwarding of organisationally confidential messages to external locations
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- Accessing copyrighted information in a way that violates the copyright
- Breaking into the organisation's or another organisation's system, or unauthorised use of a password/mailbox
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

E-mail such as passing on chain mail, jokes, spam, animations, hoax virus warnings are actively discouraged and considered inappropriate.

### **Avoiding Spam**

Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. Despite the proliferation of anti-spam solutions on the market, spam volume has reached epidemic proportions. Our Internet Service Provider enables us to manage a number of tools to prevent or reduce incoming Spam messages and can be set for individual accounts. If a staff member is experiencing incoming Spam messages, these settings should be put in place and monitored to help reduce or prevent unsolicited emails.

Individual staff member's @lgec.org.uk email addresses should not be given out without permission of the staff member. LGEC's central email address ([lgec@lgec.org.uk](mailto:lgec@lgec.org.uk)) should be used as a general email point of contact for LGEC.

### **Use of out-of-office notifications**

These notifications are usually considered as Spam messages and should therefore not be set without approval by the Chief Executive.

### **Email Signature files**

All email accounts should include the following signature information: name, job title, organisation, address, email and web addresses, company and charity number.

### **Appropriate email etiquette**

Email etiquette should be considered when writing any email, either internally or externally. Use of language and appropriate tone should be considered including no capitalisation of text, correct forms of address, spelling check and signing off.

## **3. Good housekeeping practices and password security**

Once a new email account has been set-up, the email password is documented centrally and stored securely. Email passwords should then not be disclosed under any circumstances.

## **4. Inappropriate messages**

All staff members and volunteers are prohibited to deliberately write, store or distribute inappropriate messages, for instance any that might cause offence or harassment on grounds of sex, race, disability, age, religion, including:

- Using the Internet to send offensive or harassing material to other users.
- Any potentially offensive, demeaning or inappropriate material that is received should be deleted immediately. Such mail should not be forwarded either internally or externally.

## **5. Accessing inappropriate material**

All staff members and volunteers are prohibited to deliberately access offensive, obscene or indecent material from the internet, such as pornography, racist or sexist material, violent images, incitement to criminal behaviour etc. In particular the following is deemed unacceptable use or behaviour by staff:

- Visiting Internet sites that contain obscene, hateful, pornographic or other illegal material.
- Using the computer to perpetrate any form of fraud, or software, film or music piracy.
- Hacking into unauthorised areas.
- Creating or transmit defamatory material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus into the corporate network.

## **6. Copyright and licensing restrictions**

All staff and volunteers at LGEC should be aware and comply with copyright and licensing restrictions that might apply to downloaded and forwarded material, whether Internet or e-mail, and including unauthorized software, games, magazine disc items etc.

The unintended importation of viruses is often through downloading files and programmes from external sources

The installation of some software programmes can sometimes distribute malicious code causing damage to our ICT network.

Downloading commercial software or any copyrighted materials belonging to third parties should only occur where the download is covered or permitted under a commercial agreement or other such licence.

## **7. What might happen if a breach of this policy occurs**

Unacceptable use of the LGEC's ICT resources as described in this document is strictly prohibited and may constitute a disciplinary offence.

Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures as outlined in LGEC disciplinary proceedings, such as verbal and written warnings, through to dismissal.

## **8. LGEC's ICT Network Guidelines**

All staff and volunteers are expected to follow LGEC's health and safety policy and guidelines that are issued including advise on correct seating, posture and positioning of the computer. Food and drink should be consumed carefully around PCs.

### **File management**

LGEC runs an ICT network maintained by an external contractor. All files should be saved on either:

H:/ drive: staff members own working documents and files

Z:/ drive: shared access files including organisational and project files

All personnel related files are located on the Z:/ drive and may be accessed only by the Chief Executive, Finance Manager and Projects Manager.

Sage Accounts related files including payroll files are only available to be accessed by the Chief Executive and Finance Manager.

The Chief Executive is considered "Network Administrator" and is able to manage the access of any other files on the network, in addition to being able to access all data on users H:/ drives.

Data should not be saved on any desktop C:/ drive

File names should be clearly describe the content of the document. If different versions of a draft document are created, the file name should clearly indicate e.g. "xxx proposal draft #2" or indicate whether this is the final version".

See LGEC's Data Protection Policy regarding guidelines on how long documents should be stored.

### **Staff members working from home**

All files that are worked on at home including draft documents should be copied onto the central LGEC ICT Network at the earliest available opportunity, preferably the next working day that the staff member is back on the office.

Staff members are also permitted to access the computer network on LGEC's central server when working from home via an internet connection. See the VPN instructions for further information.

### **Back-up**

An automatic backup of the ICT Network is performed every day between 10am and 4pm. At the end of each day, it is the responsibility of the Chief Executive to take this data backup drive home overnight, or nominate this task to another staff member for an agreed period. The backup drive is then brought back into the office the following morning for next day's backup. Where this is not possible, a message is flagged up advising that the day's backup was unable to take place.

Each Tuesday, the Administration Officer swaps the backup drive with the second backup drive stored in a secure location on site, to ensure a backup is always available in the building.

The data on the external backup drives includes an incremental back up over the last seven days, plus a full backup that is completed on a Monday. All data saved to the backup drive is automatically securely encrypted and does not pose a data protection risk if this data drive was stolen.

### **Security and Anti-virus**

LGEC uses anti virus software automatically set to update via the internet. If any user thinks they have a virus, this should be reported to the network maintenance contractor via the report procedure outlined below. Alternatively, the anti virus software should be ran on the computer concerned. Spy ware is also used on each desktop computer to prevent unauthorised and/or unintended data security risks occurring.

### **Troubleshooting**

If a staff member is unable to resolve an ICT related problem, this should be reported to the Administration Officer who will document the fault then liase with our external ICT contractor to resolve. If the Administration Officer is unavailable, faults should be reported to the Chief Executive to resolve in liaison with our external contractor.

Policy finalised August 2008