

# Lagan Valley Regional Park IT Policy



## Virus Control

The deliberate introduction of malicious software to a system is a criminal offence under the Computer Misuse Act 1990.

No files should be loaded on to any system from CD or USB unless they have first been virus checked by IT Services.

Floppy disks being used to send files to external users can be virus checked before they are sent. If required this can be done by IT Services.

All servers and most PCs have anti-virus software installed.

Where a virus is detected this will be reported immediately to IT Services who will attempt to “clean” and rebuild the affected PC and update the anti-virus software.

## Protection of Hardware from Accidental Damage

Care should be exercised when eating or drinking near IT equipment. Eating and drinking is not permitted near the server.

The location of all hardware (computers, printers, modems etc.) should comply with Health and Safety standards including the stability of the desk surface, and elimination of trailing cables.

All personal computers and printers should be switched off when not in use for extended periods, such as overnight or during weekends, except for the server.

Magnetic media (e.g. diskettes, tapes) should not be placed next to laser printers, photocopiers or telephones as these can cause corruption of the data on the storage media.

Diskettes/CD ROMS should be labelled and kept in boxes with sensitive diskettes stored in locked desks or fireproof safes.

Air vents on computers should not be obstructed.

## Protection of Data from Hardware Loss

Backups of data and system programmes will be taken on a regular basis as determined by the IT Manager and IT Officers.

Data should not be held locally on PCs, as this is not included in the automatic nightly backup of the network servers. Data should be saved to files on the servers.

Backup media will be stored securely off-site.

Backup recovery procedures will be tested on a regular basis as determined by the IT Manager and IT Officers.

## Protection of Data from Unauthorised Access

Password controls must be implemented. Passwords should have the following characteristics...

- Be at least 5 characters long
- Contain letters and numbers
- Be different from the previous passwords used
- Be user generated

Passwords should be changed...

- At least once every 40 days

System password details are recorded by the IT Officers and kept securely.

Password Protected Screen Savers may be used if required but passwords for screen savers must be notified to IT Services so that access to the PC can be gained if maintenance is required.

New floppy disks should be used when transferring data to outside organisations.

All storage media, including backups, should be clearly marked to avoid confusion over their contents.

## Software Control

All software must be purchased through IT Services and no software (including evaluation software) should be installed without permission from IT Services.

A register of software will be maintained by the IT Officers.

Software must not be copied, as this is an infringement of copyright and therefore illegal - unless specifically permitted by the licensing agreement. This includes loading the software from one set of disks onto several PC's.

All System Software disks will be stored securely in the IT Server Room. These are the only proof of a legal license to use the software, and may be required to be produced in evidence should the Federation Against Software Theft (FAST) investigate.

## Special Considerations for the use of Portable Computers

All previous policy statements apply to portable computers and the following special considerations, as by their nature portable computers are the most vulnerable to theft or loss.

Portable computers should not be left unattended i.e. in a car, hotel room, office or even at home.










Backups should be taken and stored securely of all sensitive information.

Passwords should be used on sensitive information wherever possible.

Laptop theft is the most common security breach – if confidential data is going to be stored on a laptop IT Services should be consulted as to how to correctly store the data

## Using the Internet

**Use of the Internet by volunteers that can be deemed to be of an illegal, offensive or unethical nature is unacceptable.**

-  Violation of copyright, license agreements or other contracts for example copying and using software for business purposes from a site where there is a clear limitation for personal use only;
-  Downloading or viewing any information which could be considered illegal or offensive e.g. pornographic or racist material;
-  Successful or unsuccessful attempts to gain unauthorised access to information resources - commonly known as 'hacking';
-  Using or knowingly allowing someone else to use any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises or representations;
-  Without authorisation destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the availability and/or integrity of computer-based information and/or information resources;
-  Without authorisation invading the privacy of individuals or entities that are creators, authors, users or subjects of the information resources; for example reading the e-mail of another without permission;
-  Using the Internet for political lobbying;
-  Transmitting or causing to be transmitted, communications that may be construed as harassment or disparagement of others; and
-  Violating any UK laws pertaining to the unauthorised use of computing resources or networks.

**Personal use of the Internet should only be during volunteer's free time and should always take second place to the carrying out your volunteer role.**

It is not acceptable for resources and, in particular, volunteers time to be wasted in casual surfing/browsing of the Internet. However, personal use is permitted provided all guidelines within this document are adhered to,

accesses are minimised and are of a specific nature (as opposed to casual and aimless browsing), i.e. directed to a specific Web page or a particular subject matter.

## Downloading of Files & Software

No file should be downloaded from or via the Internet unless doing so is expressly permitted by the IT Manager and it is in connection with the user's job.

Particular attention must be paid to any specified licensing specifications or other similar conditions. Volunteers are not permitted to enter into any agreement on behalf of the LVRP.

Where permission to download is not explicit to do so could be deemed to be 'hacking' or in breach of copyright laws and expose the LVRP to civil and criminal liabilities should also avoid downloading large files (> 1 Mb). If you need a large file downloaded, speak to your supervisor.

## Use of E-Mail

### Introduction

Increasingly e-mail is being seen as the preferred mechanism for communicating not only internally within an organisation but also externally to other organisations outside the LVRP. While it would be foolish to ignore the obvious advantages to all parties in using this technology, particularly in view of the fact that others external to this organisation initiate many contacts using this method, volunteers must accept the need to be professional in approach whenever communicating externally, irrespective of the medium.

Unlike other forms of communication there are also special security issues with e-mail including the inadvertent introduction of computer viruses and the danger of messages being read by other than the intended recipient. This is particularly so for e-mail that may be sent or received via less secure networks such as the Internet.

### Outgoing Email - Tone and Content

Writing a letter and having it typed on headed notepaper almost automatically instils a 'formality of tone' on the author, and this is a good thing (but not forgetting the spirit of the 'Plain English' campaign). However, e-mail almost has the exact opposite effect. Tone and content tend to be much more relaxed and humour can be the norm and this is not necessarily a good thing when dealing with outsiders. **Email is not a written telephone conversation.** It is difficult to put a laugh into your words even if you were smiling when you wrote them!

Care too needs to be taken when responding to an e-mail. The tone of response is often dictated by the tone of the originating message, nevertheless, without being bureaucratic or stilted or needlessly formal, frivolous e-mail should be avoided even where the original message may itself appear to be frivolous.

### Outgoing E-Mail - Security

The route by which e-mail is delivered is often circuitous and may even involve being exposed to very insecure networks. Users should remember that e-mail messages can be intercepted due to the nature of the internet. It is possible to set up routines that can scan passing e-mail for key words without being detected - the Internet equivalent of phone tapping. Consequently, volunteers should give very serious consideration to the contents of any message or attachments sent by e-mail.

The content of e-mail is subject to all applicable UK laws such as those relating to copyright, defamation, data protection and public records, as well as statutes concerning the sensitive and contentious issue of pornography. Obviously nothing illegal or infringing a third party's intellectual property rights should be included in an email.

### Checking for Viruses

The main text of an e-mail message **cannot** contain a virus.

Any attachments to an e-mail message **can** contain a virus and volunteers must take care when dealing with these. Provided all PCs within LVRP contain anti-virus software volunteers can assume that any attachments to email messages originating internally are virus-free. However, there is no guarantee that attachments to mail received from outside the LVRP are similarly safe. Remember that the developers and suppliers of anti-virus software are, of course, always at least one step behind the creators and distributors of viruses.

*Volunteers should note that while the automatic anti-virus software is able to detect and can subsequently delete viruses, through either "cleaning" the attachment or removing the attachment altogether. Users should be aware that attachments containing viruses can damage not only the host PC but potentially also the server. This will result in disruption to the work of the PC's 'owner' and create additional and avoidable work for IT Services.*

A particularly dangerous type of virus is that known as a Trojan horse. These can arrive as e-mail attachments and, indeed, are often attached to e-mail claiming to enhance security. Typical actions by this type of virus include the deletion of files on the hard disc but, some can locate the user's password, and anything else, by following keystrokes - a technique known as 'sniffing'. The sniffed data is then sent back to the hacker via e-mail.

While there is defence against these Trojan horses volunteers can at least take steps to reduce the likelihood of introducing viruses of any description by following the procedures contained in the policy.

**Particular attention should be given to attachments from unknown or dubious sources. Where there is doubt or suspicion, advice should be sought from IT Services before any such attachment is opened.**

## Reporting Viruses

The virus scanning software will automatically notify the user of any virus discovered in an attachment.

However, sometimes mail messages themselves (not to be confused with the attachments) claim to warn of viruses and in such cases volunteers must pass the mail message itself, using e-mail, to the IT Manager. There have been some cases, although not always, in which such warnings have been hoaxes that nevertheless waste time and effort and cause unnecessary panic if passed on to others. Volunteers must, therefore, only pass on such warnings to the IT Manager and not to any others either within or external to the LVRP.

## 1998 DATA PROTECTION ACT (SUMMARY)

The principles of protection of Personal Data are contained within the Data Protection Act 1998 covering both computerised and manual data. These impose specific requirements on LVRP volunteers when handling Personal Data. These principles are:

### First Principle

**Personal data shall be processed fairly and lawfully.**

### Second Principle

**Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

### Third Principle

**Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

### Fourth Principle

**Personal data shall be accurate and, where necessary, kept up to date.**

### **Fifth Principle**

**Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.**

### **Sixth Principle**

**Personal data shall be processed in accordance with the rights of data subjects under this Act.**

### **Seventh Principle**

**Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

### **Eighth Principle**






**Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data..**

When handling Personal Data, volunteers must be aware of, and adhere to, these principles particularly with regard to passing data on to other users.






**If in doubt check with the IT Manager.**

## **IMPORTANT DO'S AND DON'TS**

### **DO**







-  Check all floppy disks for Viruses
-  Save all documents to appropriate server
-  Store your backups and system disks securely off site
-  Change your confidential passwords regularly
-  Report Information Technology Security Breaches to the IT Manager

## DON'T

-  Leave your PC switched on overnight or unattended for long periods of time
-  Save files locally on PC hard drive
-  Load software – any software requirements must be coordinated by IT Services
-  Remove hardware without notification of the IT Manager
-  Use Personal Data unless you are sure that it is in compliance with the Data Protection Act (if in doubt check with the IT Manager)

**For more information contact IT Services.**

## USE OF E-MAIL - THE POLICY

1. The E-Mail system must not be used to:
  -  transmit obscene, offensive or damaging material;
  -  transmit threatening material or material intended to frighten or harass;
  -  transmit defamatory material;
  -  infringe copyright;
  -  transmit unsolicited advertising or similar activities;
  -  attempt unauthorised access to other networks or systems.
2. Volunteers should restrict the recipients of e-mail messages to those who actually may have interest in the message contents. The occasional general interest message or query to all for example is permitted but on-going e-mail conversations, which may be of little interest to many of the recipients, should be restricted.
3. Volunteers should check e-mail inboxes at least daily and provide responses appropriate to the importance of the message.
4. In order to ensure an efficient service unwanted messages should be deleted.
5. Volunteers have the ability to protect their own e-mail account through the use of passwords and should use this facility using passwords not easily detectable. Volunteers will be held accountable for all e-mails originating

from their own account, therefore password protection is of utmost importance.

6. Unauthorised access to other users' e-mail accounts is prohibited.
7. E-mail messages must be clear and concise and, for external messages, tone and content must be suitable for a business communication and appropriate to the medium.
8. Formal communications i.e. where otherwise a LVRP-headed letter may have been used, should be printed and filed, along with any attachments, in the appropriate Registered File.
9. No passwords of any description may be transmitted via e-mail.
10. In order to ensure appropriate corrective action is taken, and no unnecessary panic is caused by hoaxes, volunteers must report any virus incidents immediately, or any other apparent breach in security, to the IT Security Officer. Volunteers must not take it upon themselves to issue warnings to volunteers within or outside the LVRP.
11. Personal use of E-mail is permitted provided the above rules and guidelines are followed, such personal use is restricted to volunteers' free time and is kept to reasonable levels. Volunteers are also instructed to include the disclaimer below in all personal e-mail:

***“This e-mail is a personal communication and is not authorised by or sent on behalf of any other person or the LVRP”***

Abuse of this privilege will result in its withdrawal and possible disciplinary action against the volunteers concerned.

12. Failure to comply with this policy may result in disciplinary action.