



for a stronger third sector

Technology Handbook

Organisation _____

Address _____

Telephone _____

Email _____

Website _____

Handbook maintained by _____



Technology handbook

1	Organisation	9
1.1	Description.....	9
1.2	Mission statement.....	9
1.3	Strategy	10
1.4	Staff numbers	10
1.5	Turnover	11
1.6	Budget	11
1.7	Responsibilities.....	12
1.8	Our Documents	13
2	Compliance.....	15
2.1	Health & Safety.....	15
2.1.1	H&S risk assessments.....	15
2.1.2	Electricity at Work.....	16
2.2	Accessibility	16
2.3	Data Protection Act (DPA) registration	17
2.4	Copyright Acts	17
2.5	Waste Electrical and Electronic Equipment (WEEE)	18
2.6	Insurance Policy	19
2.7	Our Compliance documents	20
3	Inventory	21
3.1	Hardware Audit.....	21
3.2	Software audit.....	23
3.3	Our Inventory documents	24
4	Configuration	25
4.1	Password Safe	25
4.1.1	Product Keys	26
4.2	Server Configuration.....	26
4.2.1	Users and Groups	27
4.2.2	Resources	28
4.2.3	Applications	28
4.3	Network	28
4.4	Local Area Network	29
4.4.1	Network Diagram.....	29
4.4.2	IP Address map.....	29
4.4.3	Wireless Access	30
4.5	Wide Area Network (WAN)	31
4.5.1	Router configuration	31
4.5.2	Firewall configuration.....	32
4.6	Internet services	32
4.6.1	Domain Name Registration	32
4.6.2	Extract from Nominet.....	34
4.6.3	Email	34
4.6.4	Website	35
4.6.5	Web server hosting.....	36
4.6.6	FTP Server	37
4.6.7	Mailing list.....	38
4.6.8	Social media.....	39
4.6.9	Cloud services	40

4.6.10	Spam/virus filtering service.....	41
4.7	Our documents	42
5	Contracts	43
5.1	Service contract	43
5.2	Support contract	44
5.3	Maintenance contract	45
5.4	Broadband (Internet Access Provider).....	46
5.5	Internet Service Provider (ISP)	47
5.6	Online service subscriptions	48
5.7	Hardware, software and consumables supplier accounts.....	49
5.8	Our Contract documents.....	50
6	Policies	51
6.1	Disaster Recovery Policy	51
6.2	Technology purchasing Policy	51
6.3	Acceptable Use Policy	52
6.4	Training Policy	52
6.5	Social Media policy	53
6.6	Electronic Monitoring	53
6.7	Firewall Policy.....	54
6.8	Data Protection policy	55
6.9	Our Policy documents.....	56
7	Procedures	57
7.1	Business Continuity	57
7.2	Technology user induction.....	57
7.3	Support and housekeeping.....	58
7.4	Backup.....	58
7.5	Our documents	59
8	Appendices.....	61
8.1	Technology Healthcheck	61
8.2	Sources of help.....	61
8.3	Sources of advice	61
8.4	Further resources and publications	61

Introduction

Who is this handbook for?

This handbook is designed to be a central repository of all information relevant to the configuration and management of the technology services within an organisation.

It is aimed at voluntary sector staff with responsibility for supporting, developing, managing and securing technology systems. This will vary according to the size and complexity of an organisation so could be an accidental techie, technology manager, trustee or volunteer. Whoever it is, the handbook should help in the smooth running of the systems.

What are the benefits of using the handbook?

- allows technology issues to be tackled methodically rather than piecemeal
- easily identify missing information - backup discs, licence keys, insurance, etc
- better plan and manage technology for the future
- help an organisation to gather information required as part on a technology healthcheck
- assists support staff, both internal and external, to easily access vital information when troubleshooting or upgrading

The handbook is designed to be a document that is continually maintained and updated as the technology system changes.

What does this handbook not do?

- it is not a user guide
- it is not instructional
- it does not replace skilled or experienced technology staff



knowledgebase

Where appropriate, links have been inserted to articles on the Lasa ICT knowledgebase to provide more information on the topic. The knowledgebase also has an extensive plain English glossary of terms in case there are some here that you are not familiar with – just use the Search facility.

Feedback

Lasa welcomes feedback on this handbook which should be seen as a work-in-progress Please email us at ist@lasa.org.uk

Credits

The Technology Handbook was originally devised by Mike Veitch of The Helpful Helpdesk (www.helpfulhelpdesk.org.uk) aided and abetted by members of the UKRiders mailing list (<http://lists.lasa.org.uk/lists/info/ukriders>) with further input from members of the Information Systems Team at Lasa (www.lasa.org.uk/ict). Following a trial period, it has been further revised and added to by Lasa.

Licensing

This work is licensed under a Creative Commons Attribution-noncommercial-NoDerivs 3.0 License www.creativecommons.org/licenses/by-nc-nd/3.0

Version

This is version 1.0 – May 2011.

1. Organisation

1 Organisation

Section 1 should contain a brief description of what the organisation actually does and will help those giving you support align their services with your priorities.

1.1 Description

Here you should summarise your organisation in a paragraph. This will give support staff a general overview of your organisation.

? Can you describe your organisation?

Please enter a paragraph below:



1.2 Mission statement

Many organisations have a formal, short, written mission statement that describes their purpose.

? Do we have a mission statement?

If yes, enter it below:



If no, bring this to the attention of your local management.

1. Organisation

1.3 Strategy

The overall direction of technology within an organisation is guided by a technology strategy. This helps ensure that the purchase and use of technology is firmly tied to the organisation's aims and business and help make the best use of their technology resources now and in the future.




knowledgebase – A technology strategy framework
<http://www.ictknowledgebase.org.uk/itstrategyframework>



Do we have a technology strategy?

If yes, please add it to the end of this section or state location



If no, bring this to the attention of your local management.

1.4 Staff numbers

It is useful to record how many staff and volunteers (full time equivalent - FTE) you have who are using technology in any way?



How many staff (FTE) do we have?



1. Organisation

1.5 Turnover

It is useful to record your current total annual financial turnover is this is related to any technology budget you might have.

? What is our annual turnover?



1.6 Budget

Running effective technology within an organisation is a significant cost of and must be managed.



knowledgebase – Calculating your technology budget

<http://www.ictknowledgebase.org.uk/calculatingtechnologybudget>

? Do we have a technology budget?

If yes, please add it to the document section or enter location below



If no, bring this to the attention of your local management.

1. Organisation

1.7 Responsibilities

All organisations need to make decisions and all have different processes for arriving at a decision. However it is common for individuals to be responsible for decisions.



knowledgebase – Staff responsibility for IT support

<http://www.ictknowledgebase.org.uk/responsibilityforsupport>



Who has responsibility?

This means the individual has the authority to act on behalf of the organisation.

Area of responsibility	Name
------------------------	------

Technology configuration	
--------------------------	--

Technology support	
--------------------	--

Strategy	
----------	--



Purchasing	
------------	--

Policy and procedure	
----------------------	--

Security	
----------	--

Data Protection	
-----------------	--

You may wish to add to areas of responsibility to this list

1. Organisation

1.8 Our Documents

You should list the documents you have added to this handbook for reference. If the document is not in the handbook then you should give the location and who maintains the document. (The first entry is an example)

<i>Section Ref</i>	<i>Document Description</i>	<i>Maintained by</i>
<i>1.2</i>	<i>Mission Statement</i>	<i>Trustees</i>

2. Compliance

2 Compliance

Section 2 will help you compile the evidence you require to demonstrate your organisation is complying with relevant legislation. The list is not exhaustive and your organisation may have other legislative requirements not listed in this section.

2.1 Health & Safety

As a minimum requirement your organisation must comply with the law. The operation of technology systems is not a hazardous environment. There are some specific requirements relating to the use of technology equipment in offices.

2.1.1 H&S risk assessments

Employers have a responsibility to ensure compliance with current Health and Safety legislation in particular you should:

- Analyse workstations, and assess and reduce risks
- Ensure workstations meet minimum requirements
- Plan work so there are breaks or changes of activity
- On request arrange eye tests, and provide spectacles if special ones are needed
- Provide health and safety training and information

Further information can be obtained from the publication *Working with VDUs* published by the HSE (www.hse.gov.uk/pubns/indg36.pdf)



knowledgebase – Computer health and safety

www.ictknowledgebase.org.uk/healthandsafety



Have we done any technology related H&S assessments?

If yes, please add it to the document section or enter location below



If no, bring this to the attention of your local management.

2. Compliance

2.1.2 Electricity at Work

The Electricity at Work Regulations 1989 requires precautions to be taken against the risk of death or personal injury from electricity in work activities. In the main, the Regulations are concerned with the prevention of danger from shock, burn, explosion or arcing or from fire initiated by electric energy.

To ensure a safe working environment all electrical equipment should be periodically tested. This is usually called PAT (Portable Appliance Testing) and many companies will want to come and test your IT equipment annually and charge you a fee for each item tested. Before you waste too much of your organisation's money make sure you read the leaflet *Maintaining Portable Electrical Equipment in offices and other low-risk environments* published by the HSE (<http://www.hse.gov.uk/pubns/indg236.pdf>)



Do we have a PAT log?

If yes, please add it to the document section or enter location below



If no, bring this to the attention of your local management.

For most organisations the maintenance of the installation (that is the sockets and light fittings) will be the responsibility of the landlord, but you should check. If you have this responsibility you should engage the services of an electrical contractor.

2.2 Accessibility

Assistive technologies make your services and information more accessible to wider groups of people and your technology more accessible to enable staff to be more productive. People with disabilities and literacy issues will gain the most benefit from available technologies with a little awareness and planning.



knowledgebase – Accessibility and inclusion

www.ictknowledgebase.org.uk/accessibilityinclusionbasics

2. Compliance

? Have we done any technology related accessibility assessments?

If yes, please add it to the document section or enter location below



If no, bring this to the attention of your local management.

2.3 Data Protection Act (DPA) registration

If your organisations keep records of personal details of identifiable individuals you will probably need to register (notify) as a Data Controller with the Information Commissioners Office.

You can check your registration online at

www.ico.gov.uk/ESDWebPages/search.asp



knowledgebase – Introduction to the Data Protection Act

www.ictknowledgebase.org.uk/dataprotectionactintroduction

? Are we registered to hold personal data?

If yes, you should complete this section



Registration Number:

Data Controller:

Date Registered:

Registration Expires:

If no, you should check that you do not require to register.

2.4 Copyright Acts

Stealing is crime; no one likes to have their things taken from them and used without their permission. Intellectual Property (IP) is owned too and you must have the owner's permission to use it. It is important that if you are using someone else's IP, you can show you have their explicit permission to use it.

2. Compliance

? Are we using copyrighted material?

If yes, where do we keep letters of authorisation?



If no, bring this to the attention of your local management.

For more on IP you can visit the Intellectual Property Office

www.ipo.gov.uk/copy.htm

2.5 Waste Electrical and Electronic Equipment (WEEE)

The WEEE directive came into effect on July 1st 2007. It was introduced in an attempt to reduce the amount of electrical waste heading to landfill and has significant implications for producers of electrical items and any non-household users of electrical items.

The list of equipment covered by the directive is extensive so a simple rule to follow is “if it has a plug then the directive applies”.

If your organisation is disposing of technology equipment, before throwing it out you should investigate donating to a company that will reuse the equipment. There are many charities that provide collection services (although you may be charged per item).

If you dispose of any equipment under the WEEE directive make sure to obtain paperwork from the waste management contractor.



knowledgebase – Disposing of old computer equipment

www.ictknowledgebase.org.uk/disposingoftechnology

? Are we complying with the WEEE directive?

If yes, please add it to the document section or enter location below



If no, bring this to the attention of your local management.

2. Compliance

2.6 Insurance Policy

Technology equipment is particularly vulnerable to theft either from your premises or while your equipment is out of the office. Your organisation should ensure that you have a level of cover that will ensure you don't lose out should the worst happen.

Some insurance cover for all risks can be prohibitively expensive and therefore may restrict the ways you can utilise your technology equipment.

If your organisation gives technology (or any other) advice you should check that this is covered under your organisation's Professional Indemnity Policy.

? Do we have an all risks policy for IT equipment?

If yes, you should complete this section

Insurance company:

Policy Number:

Renewal date:

Agent:



List any significant policy exclusions:

If no, you should periodically review your insurance needs.

? Do we have Professional Indemnity insurance for advice that we give?

If yes, you should complete this section

Insurance company:

Policy Number:

Renewal date:

Agent:



List any significant policy exclusions:

If no, you should periodically review your insurance needs.

2. Compliance

2.7 Our Compliance documents

You should list the documents you have added to this handbook for reference. If the document is not in the handbook then you should give the location and who maintains the document. (The first entry is an example)

<i>Section Ref</i>	<i>Document Description</i>	<i>Maintained by</i>
1.4	DPA registration extract	J. Latimer

3. Inventory

3 Inventory

This section gathers together all the information about the equipment you own or lease. It also where you keep all the information about the software you have purchased or used within your organisation.

The process of gathering this information is called an audit. The audit can be conducted manually or can be completed using software tools to help automate the process:

e.g. Belarc Adviser (http://www.belarc.com/free_download.html), and SpiceWorks (<http://www.spiceworks.com>).

3.1 Hardware Audit

The hardware inventory is kept for a number of reasons:

- Inclusion of items in the Assets Register
- Insurance (replacement)
- Upgrade suitability

There are many tools available that can help you compile a Hardware Inventory or you could just use a spreadsheet.

Hardware that should be included in an inventory includes servers, PCs, laptops, printers, routers, hubs, switches, firewall, wireless access points, UPS etc

For all hardware include purchase date, price, supplier, manufacturer, model name/number, serial number, warranty information, brief specification (e.g. for PCs CPU, RAM, hard drive capacity)



knowledgebase – Sample ICT Inventory

www.ictknowledgebase.org.uk/sampleinventory



Do we use tools to compile our hardware inventory?

If yes, please enter the name of the tool used below



If no, you should seek advice.

3. Inventory

? Do we have a hardware inventory?

If yes, please add it to the document section or enter location below



If no, bring this to the attention of your local management.

? If we have a hardware inventory who maintains it?

If yes, enter the name of the person with responsibility



If no, bring this to the attention of your local management.

3. Inventory

3.2 Software audit

The software inventory is kept for a number of reasons

- To know exactly what software is installed and in use
- To track the versions of software in use
- To enable accurate rebuilds after disaster
- To assist with licence compliance

There are many tools available that can help you compile a Software Inventory – as with hardware auditing Belarc and Spiceworks will audit your software..



Do we use tools to compile our software inventory?

If yes, please enter the name of the tool used below



If no, you should seek advice.



Do we have a software inventory?

If yes, please add it to the document section or enter location below



If no, bring this to the attention of your local management.

3. Inventory

3.3 Our Inventory documents

You should list the documents you have added to this handbook for reference. If the document is not in the handbook then you should give the location and who maintains the document. (The first entry is an example)

<i>Section Ref</i>	<i>Document Description</i>	<i>Maintained by</i>
<i>3.1</i>	<i>Hardware asset register</i>	<i>Finance Officer</i>

4. Configuration

4 Configuration

The configuration of your technology system is the way you have customised the standard or default installation of hard ware or software. Recording these changes will mean that you can always access components to make further changes or in the event of disaster fully restore your technology system.

4.1 Password Safe

It is essential that you keep all passwords securely. It is tempting if you only have one or two passwords to memorise them. However, what if you are not available when the password is required? Some systems may not let you choose a password or your chosen password may not fit with their complexity rules. To ensure that passwords are available to authorised staff when required all administrative passwords should be stored in a secure file. This can be a complex electronic file system or could as simple as small notebook in a locked drawer which is accessible if your system is down. Whichever system you use the password file must be kept in a secure location.

In addition to your main administrator password you'll probably have a number of others e.g. equipment such as Internet router, firewall; Broadband account; Internet accounts including ftp to your website; hosted services – maybe you have an organisational Flickr or YouTube account, blog etc; software license accounts such as anti-virus, anti-spam; software support sites e.g. finance or database software; VPN log ins; and so on. Make sure they are all recorded. Don't forget to note down the usernames as well.

Associated with the password file should be the policy on password recording and change control.



knowledgebase – Choosing and using secure passwords

www.ictknowledgebase.org.uk/choosingpasswords

4. Configuration



Do we have a password file?

If yes, you should complete this section

Where is it located?



Who has access to it?

If no, you should document how to recover passwords and attach to the documents at the end of this chapter.

4.1.1 Product Keys

Many of the software products installed on your server or workstations are supplied with a product key, activation code or serial number. These codes are important as they will be required to re-install the software or access online support services. All of these codes should be stored in file. This can be a complex electronic file system or could as simple as small notebook. Whichever system you use the product codes file should be kept in a secure location.



Do we have a product key file?

If yes, you should complete this section

Where is it located?



Who has access to it?

If no, you should document how to recover product keys and attach to the documents at the end of this chapter.

4.2 Server Configuration

A server is installed to meet a technology requirement. A server (or servers depending on the complexity of your system) can play a number of roles within your technology network the actual setup will depend on your original requirement. Some of the roles your server may perform include:

4. Configuration

- Security – validating user logins, giving users secure permission and access to files, anti-virus and spam filtering
- Applications – centralised software, e.g. accounts, email,
- File storage – all organisational data including documents, email, databases etc
- Printers – configuring, managing and sharing printers
- Internet – controlling access to the internet
- Backup – managing the back up regime as part of a disaster recovery plan (see 7.4)

4.2.1 Users and Groups

Groups are at the heart of user management. When a systems administrator wants to give users access to a folder, a printer or application on the server, permission is granted to a group. The systems administrator will then ensure that the user requiring access is in the group.

It is vital that the group structure that is setup on your server is recorded.



knowledgebase – Moving from personal to organisational directory structures

www.ictknowledgebase.org.uk/directorystructures



Do we have a record of the server group structure?

If yes, you should complete this section?



Where is it located?

Who has access to it?

If no, you should document the group structure.

4. Configuration

4.2.2 Resources

Users require access to resources in order to complete tasks. Resources can include anything that the systems administrator wishes to control access.



Do we have a record of the server resources?

If yes, you should complete this section

Where is it located?



Who has access to it?

If no, you should document the resource structure.

4.2.3 Applications

If your server does have the server components of client/server applications then you should list these below:



Do we have client/server applications?

If yes, you should complete this section

Name of application:

Who has access to it?



If no, you can leave this section blank.

4.3 Network

The network is a collection of components (infrastructure, hardware and software) that together allow users of the technology system to communicate with each other internally and where enabled communicate with other users and services on the Internet.

4. Configuration

4.4 Local Area Network

The Local Area Network (LAN) is the section of the network that is normally in your premises and under your control. A LAN is the infrastructure that connects together the devices on your network – it can be cabled or wireless or a mixture of the two.



knowledgebase – What is a network?

www.ictknowledgebase.org.uk/whatisanetwork

4.4.1 Network Diagram

Your network supports all the connections between workstations, printers, servers and the Internet. Whenever possible your network should be professionally installed and maintained to current network wiring standards. If this has been done the contractor will document your network and leave you with a copy.

If you do not have a network diagram you should think of getting one done for you. It will help with fault finding.



Do we have a network diagram?

If yes, please add it to the document section or enter location below



If no, you can leave this section blank.

4.4.2 IP Address map

Your network relies on every device having a unique address. This is called the Internet Protocol (IP) address and usually takes the form 192.168.x.y. It is normal for all devices to be assigned their unique IP address by a special device called a Dynamic Host Configuration Protocol (DHCP) server. In small networks the Broadband router usually acts as the DHCP server. In larger networks with a dedicated server, the server can be configured to act as the DHCP server.

4. Configuration

It is usual just to let the DHCP server and the devices to configure themselves automatically. However, sometimes it is better to allow a Systems Administrator to manually configure the IP address space as some equipment requires a fixed IP such as servers, printers, network equipment such as routers, switches and wireless access points. If you have done this you should have a document that describes how the IP address space has been allocated. Some of this information can be extracted from the DHCP server but the set intended should be documented.

Also your ADSL (broadband) router and firewall will have external fixed IPs which are provided by the Internet Service Provider (ISP). You should make a note of these as well.

? Do we have IP Address map?

If yes, please add it to the document section or enter location below



If no, you can leave this section blank.

4.4.3 Wireless Access

Many broadband routers come with an integral wireless access point (WAP). This WAP allows devices with wireless connectivity to connect to the router and the Internet or the organisations LAN (Local Area Network).

The WAP can be configured in many different ways including the application of security settings such as a Wi-Fi Protected Access (WPA) key. If you enable wireless access to your network you should have the WAP configuration documented. It's especially important to note the WPA key which will be a sequence of numbers and letters, usually generated by the device (or may be hard coded and noted on the outside of the router).

4. Configuration

? Do we have Wireless Access Point configuration documents?

If yes, please add it to the document section or enter location below



If no, you can leave this section blank.

4.5 Wide Area Network (WAN)

4.5.1 Router configuration

A router is the device that connects your private network (LAN) to the public internet (WAN). The router may be provided and configured by your broadband service provider or have been installed by a technician or staff member. Whoever installed it will have set up the router to work with your broadband connection. They will also have set permissions and administrative passwords. If your router develops a fault and needs to be replaced you will need all the original configuration information.

? Do we have router configuration documentation?

If yes, you should complete this section?

Router Model:

Router Location:

Router Administrator:

IP addresses (internal and external):

If not appended, where is the Router Configuration documentation is located :

If no, you can leave this section blank.

4. Configuration

4.5.2 Firewall configuration

Your firewall is the device that prevents unauthorised access from the Internet to your network; it can also help control your staff access to Internet services and also external access to the system via a Virtual Private Network (VPN). The configuration of the firewall will come from an organisation policy that clearly identifies activities that are permitted.



Do we have firewall configuration documentation?

If yes, you should complete this section?

Firewall device:

Firewall Location:

Firewall Administrator:

IP addresses (internal and external)



If not appended, where is the Firewall Configuration Documentation located :

If no, you can leave this section blank.

4.6 Internet services

The internet is now fully integrated into the organisational technology infrastructure but is normally provided and maintained by a number of external contractors.

4.6.1 Domain Name Registration

The identity of the organisation as it appears on the Internet is called a Domain Name and will be registered with an Internet registry. If your domain name ends in .uk your domain name will be registered with a company called Nominet www.nominet.org.uk . If it is not (such as a .org or .com then it will be

4. Configuration

registered with InterNIC www.internic.net Some organisations have a number of domain names for different services or websites – make sure you record them all and know when they are due for renewal so you don't run the risk of losing them.



knowledgebase – What's in a domain name?

www.ictknowledgebase.org.uk/whatsinadomainname



Do we have our own Domain Name(s)

If yes, you should write them in here?



If no, you should consider registering your domain name.



Is our domain registered with Nominet/Internic?

If yes, where is our user account and password stored?



If no, find out which registry keeps your domain name.

4. Configuration

4.6.2 Extract from Nominet

The information held by Nominet is published and accessible to any internet user. You should print out your own entry.

? Is our domain registered with Nominet?

If yes, add the printout to the documents in this section?



If no, then leave blank.

4.6.3 Email

There are a number of options for the provision of email to staff:

Webmail (e.g. Hotmail, Yahoo, Gmail)

POP3 or SMTP mail

Exchange server (or equivalent)

IMAP

? Do we have email accounts?

If yes, complete this section as fully as possible?

Email service type:

Email service provider:



Email accounts administrator

Email accounts:

If no, then leave blank.

4. Configuration

4.6.4 Website

Websites have a number of management functions associated with the maintenance of the website. These tasks can be undertaken by different individuals or external contractors. The task split into two distinct areas; website design and content management. Website design is usually the responsibility of the website developer and the organisation is responsible for content management.



Do we have a web site design contractor/company?

If yes, complete this section as fully as possible?

Name of company/contractor

Address

Telephone



Email

Account manager

Web Developer assigned to us:

If no, then leave blank.

You should also ensure that you have all the necessary passwords or access instructions to manage this aspect of the website and others such as blog, analysis services such as Google Analytics, wiki, Flickr, YouTube etc. You will need these if you change or terminate the contract with your developers.

Your developer may have provided you with software or other mechanisms such as access to a CMS (Content Management System) to update your website. This could include, Adobe Contribute, Microsoft FrontPage, FTP access, Wordpress, Drupal and Plone. However, there are many other tools available to update and maintain websites.

4. Configuration

? How do we add/change content on our website?

If yes, complete this section as fully as possible?

What software is used?

Where is it installed?

Who has access?

Where are the usernames?

Where are the passwords stored?

If no, then leave blank.

4.6.5 Web server hosting

The organisation's website can be hosted in a number of different ways. It is preferable that an organisation actually own and control all access to the website.

? Do we use a web hosting company?

If yes, complete this section as fully as possible?

Name of company

Address

Telephone

Email

Account manager

Web Developer

Web Content Managers/Editors

If no, then leave blank

4. Configuration

4.6.6 FTP Server

An FTP (File Transfer Protocol) server allows users to upload or download files using freely available FTP clients (such as WS-FTP, SmartFTP or the open source FileZilla).



Do we use an FTP Server?

If yes, complete this section as fully as possible?

Name of company

Address

Telephone

Email



Web interface address:

Administrative user account:

Where is the password?

If no, then leave blank

4. Configuration

4.6.7 Mailing list

A mailing list server (sometimes called listservs) maintains a list of email addresses for the distribution of email to the list members (similar to Yahoo Groups or Google Groups). List servers can be set up to require a minimum of administration but few require none. An organisation may also use specialist bulk mailing services for producing and distributing communications such as newsletters (e.g. CTTM@il – www.ctt.org).



knowledgebase – An introduction to email mailing lists

www.ictknowledgebase.org.uk/emailmailinglists



knowledgebase – Choosing bulk email software

www.ictknowledgebase.org.uk/bulkemailsoftware



Do we use any mailing list services?

If yes, complete this section as fully as possible?

Name of company

Address

Telephone

Email

Web interface address:

Administrative user account:

Where is the password?

Date of contract renewal

If no, then leave blank.

4. Configuration

4.6.8 Social media

Your organisation may have accounts with various social media services (such as Twitter, Facebook, Flickr, YouTube).



knowledgebase – An introduction to social media

<http://www.ictknowledgebase.org.uk/introductiontosocialmedia>



Do we use any social media services?

If yes, complete this section as fully as possible?

(1) Service name:

Web interface address:

Administrative user account:

Where is the password?

(2) Service name:

Web interface address:

Administrative user account:

Where is the password?



(3) Service name:

Web interface address:

Administrative user account:

Where is the password?

(4) Service name:

Web interface address:

Administrative user account:

Where is the password?

If no, then leave blank.

4. Configuration

4.6.9 Cloud services

Organisations are now choosing to use more services which are hosted on the internet in the cloud (also known as Software as a Service – SaaS).

Examples include online backups, Google mail, docs and calendar, Skype, Dropbox, Salesforce, Evernote and Eventbrite.



knowledgebase – Cloud Computing 101

www.ictknowledgebase.org.uk/cloudcomputing101



Do we use any cloud services?

If yes, complete this section as fully as possible

(1) Service name:

Web interface address:

Administrative user account:

Where is the password?

(2) Service name:

Web interface address:

Administrative user account:

Where is the password?



(3) Service name:

Web interface address:

Administrative user account:

Where is the password?

(4) Service name:

Web interface address:

Administrative user account:

Where is the password?

If no, then leave blank.

4. Configuration

4.6.10 Spam/virus filtering service

Much of email sent to your organisation will be spam (unsolicited email). Tools may be installed on your servers or workstations to filter spam; alternatively you may subscribe to an external service to prevent spam reaching your network. . The service may also filter mail for known viruses.



knowledgebase – Spam – solutions, anyone?

www.ictknowledgebase.org.uk/spamsolutions



Do we use a spam filtering service?

If yes, complete this section as fully as possible

Name of company

Address

Telephone



Email

Web interface address:

Administrative user account:

Where is the password?

If no, then leave blank.

5. Contracts

5 Contracts

Your technology infrastructure may be supported through contracts and SLA (Service Level Agreements) with external companies or organisations. These documents contain important information that may be required to resolve problems or conflicts. They must be held securely but easily located when required.

5.1 Service contract

If your organisation has technology services provided by a third party then this will be governed by a service contract or service level agreement. This would be the case in a resource centre were tenants were provided with IT services.



Do we have a service contract?

If yes, complete this section as fully as possible

Name of company

Address

Telephone

Website

Email

Fax

Account manager

Date of renewal:

If no, then leave blank

5. Contracts

5.2 Support contract

If you manage your own technology services but do not retain staff to manage the system then you will probably have a support contract.



knowledgebase – Working with an IT support company

<http://www.ictknowledgebase.org.uk/workingwithsupportcompanies>



knowledgebase – What to expect from a support contract

www.ictknowledgebase.org.uk/whattoexpectfromsupport



Do we have a support contract?

If yes, complete this section as fully as possible?

Name of company

Address

Telephone

Website

Email

Fax

Account manager

Date of renewal:

If no, then leave blank

5. Contracts

5.3 Maintenance contract

If you manage your own technology services and have in house expertise to provide for your support needs then you may have a maintenance contract to cover the essential hardware components of your system, such as printers.



Do we have a maintenance contract?

If yes, complete this section as fully as possible?

Name of company

Address

Telephone

Website

Email

Fax

Account manager

Date of renewal:

If no, then leave blank

5. Contracts

5.4 Broadband (Internet Access Provider)

The physical connection to the Internet is usually supported by a broadband (ADSL) service from a telecoms company.

? Do we have a broadband contract?

If yes, complete this section as fully as possible?

Name of company

Address

Telephone

Website

Email

Account manager

Date of renewal:

If no, then leave blank

5. Contracts

5.5 Internet Service Provider (ISP)

Access to the Internet is normally obtained through a contract with an ISP this could be the same company providing your Internet access.



Do we have an ISP?

If yes, complete this section as fully as possible

Name of company

Address

Telephone

Website

Email

Account manager

Date of renewal:

If no, then leave blank

5. Contracts

5.6 Online service subscriptions

Your organisation may subscribe to online services (such as spam and anti-virus filtering, mailing lists etc).

? Do we have online service contracts?

If yes, complete this section as fully as possible

Service:

Name of company

Address

Telephone

Website

Email

Account manager

Date of renewal:



Service:

Name of company

Address

Telephone

Website

Email

Account manager

Date of renewal:

If no, then leave blank

5. Contracts

5.7 Hardware, software and consumables supplier accounts

Your finance officer may set up accounts with approved suppliers.

? Do we have an approved supplier?

If yes, complete this section as fully as possible?

Hardware supplier:

Name of company

Address

Telephone

Website

Email

Account manager

Software supplier:

Name of company

Address

Telephone

Website

Email

Account manager

Consumables supplier:

Name of company

Address

Telephone

Website

Email

Account manager

If no, then leave blank

6. Policies

6 Policies

Your organisation may have agreed policies in order to avoid negative effects in the organisation, or to seek some positive benefit.

6.1 Disaster Recovery Policy

A disaster recovery policy may be incorporated within your organisation's Business Continuity Plan (see 7.1).



Do we have a Disaster Recovery policy?

If yes, please add a copy to the end of this section or state location.



If no, please raise this with your management

6.2 Technology purchasing Policy

Your organisation may consider factors other than price and delivery when selecting suppliers. Local, environmental or ethical suppliers may be preferred were available.



Do we have a technology purchasing policy?

If yes, please add a copy to the end of this section or state location.



If no, please raise this with your management

6. Policies

6.3 Acceptable Use Policy

Your organisation will have an Acceptable Use Policy (AUP) which will describe in detail how the technology system may be used and what is explicitly prohibited. It is common practice for organisations to require staff and volunteers to sign a copy of the AUP before allowing access to the technology services.



knowledgebase – ICT Acceptable Use Policies

www.ictknowledgebase.org.uk/acceptableusepolicy



Do we have an acceptable use policy?

If yes, please add a copy to the end of this section or state location.



If no, please raise this with your management

6.4 Training Policy

Your organisation will have a policy to review appropriate training needs and budget in place to keep staff up to date.



knowledgebase – How to develop an IT training policy

www.ictknowledgebase.org.uk/ittrainingpolicy



knowledgebase – Training Needs Analysis

www.ictknowledgebase.org.uk/trainingneedsanalysis



Do we have a training policy?

If yes, add the procedures relevant to technology to the documents in this section



If no, this should be reviewed by the management as a priority.

6. Policies

6.5 Social Media policy

This policy sets out the standard of behaviour expected in representing the organisation online.



knowledgebase – Social media guidelines

www.ictknowledgebase.org.uk/socialmediaguidelines



Do we have a social media policy?

If yes, add the procedures relevant to technology to the documents in this section



If no, this should be reviewed by the management as a priority.

6.6 Electronic Monitoring

It is possible to log (record) all activity within a technology system. This can include:

- login/logout times
- all emails sent or received
- all web pages visited
- all workstation activity

It is good practice and may be a legal requirement to inform staff of the level of monitoring conducted by your organisation.



Do we undertake any electronic monitoring?

If yes, please add a copy to the end of this section or state location



If no, please leave blank

6. Policies

6.7 Firewall Policy

As part of the AUP some activities may be restricted by the network service through the use of a firewall. For example the AUP may not permit users to access social networking sites. This can be prevented through configuring the firewall in line with a firewall policy.



Do we have a firewall policy?

If yes, please add a copy to the end of this section or state location.



If no, please leave blank

6. Policies

6.8 Data Protection policy

A Data Protection policy is not about explaining Data Protection; there are plenty of places you can find more information (see 2.2). It is about setting down the decisions your organisation has made about how it will comply with its legal responsibilities, and about making sure that everyone in the organisation knows what their individual responsibilities are.

Data Protection is important, not because it is about protecting data, but because it is about protecting people. People can be harmed if their data is misused, or if it gets into the wrong hands, through poor security or through careless disclosures. They can also be harmed if their data is inaccurate or insufficient and decisions are made about them, or about what services to provide them with.



knowledgebase – Data Protection policy (you can download a framework policy with model clauses)

www.ictknowledgebase.org.uk/dataprotectionpolicies



Do we have a data protection policy?

If yes, please add a copy to the end of this section or state location.



If no, please leave blank

6. Policies

6.9 Our Policy documents

You should list the documents you have added to this handbook for reference. If the document is not in the handbook then you should give the location and who maintains the document. (The first entry is an example)

<i>Section Ref</i>	<i>Document Description</i>	<i>Maintained by</i>
6.3	Acceptable Use Policy	HR officer

7. Procedures

7 Procedures

7.1 Business Continuity

If your organisation has prepared a Business Continuity Plan a component of this will be a set of procedures relating to technology services. This handbook may provide information relevant to the BCP procedures. You will need to carry out a risk assessment which will inform the plan.



knowledgebase – ICT Risk Assessment (contains a risk assessment framework)

www.ictknowledgebase.org.uk/riskassessment



Do we have a Business Continuity Plan?

If yes, add the procedures relevant to technology to the documents in this section



If no, this should be reviewed by the management.

7.2 Technology user induction

Each organisation has tailored their technology system to meet specific requirements and methods of operation. New staff should be familiarised with the technology system as part of their induction process.



knowledgebase – technology Induction manual

www.ictknowledgebase.org.uk/inductionmanual



Do we have an induction procedure for new staff/volunteers?

If yes, add the procedures relevant to technology to the documents in this section



If no, this should be reviewed by the management.

7. Procedures

7.3 Support and housekeeping

When things don't go as planned due to a hardware breakdown, software glitch or network connection issue you'll need a procedure for staff and volunteers to follow – who to initially contact, who escalates it to your support company if it can't be sorted in house, how it's recorded and monitored. You might also want to have a procedure for housekeeping which can assist in keeping support calls at bay.



knowledgebase – Good housekeeping

www.ictknowledgebase.org.uk/maintenancetips



Do we have a support and housekeeping procedure?

If yes, add the procedures relevant to technology to the documents in this section



If no, this should be reviewed by the management as a priority.

7.4 Backup

All organisations must be able to restore the technology system to a known state in the event of disaster. The procedures for recovery are part of the Business Continuity Plan but will rely on backups being available.



knowledgebase – Developing a backup strategy

www.ictknowledgebase.org.uk/backupstrategy



Do we have a backup procedure?

If yes, add the procedures relevant to technology to the documents in this section



If no, this should be reviewed by the management as a priority.

7. Procedures

7.5 Our documents

You should list the documents you have added to this handbook for reference. If the document is not in the handbook then you should give the location and who maintains the document. (The first entry is an example)

<i>Section Ref</i>	<i>Document Description</i>	<i>Maintained by</i>
7.1	<i>Business continuity plan</i>	<i>Director</i>

8. Appendices

8 Appendices

8.1 Technology Healthcheck

A technology healthcheck can be a good starting point to help you understand your technology system and what needs to be done to keep it in shape. Many consultants offer a healthcheck service and Lasa offer a template that can be used – see <http://bit.ly/dAed3S>

8.2 Sources of help

Help is all around; getting is just a matter of asking the right question to the right person. Knowing how to ask the question and finding the right person to ask is the hard part. When you need help, try to follow a logical path to solve your problem rather than a haphazard approach.

Lasa maintain the  **knowledgebase** which will help with most of your queries about technology – see www.ictknowledgebase.org.uk.

TechSoup is a US website similar to the knowledgebase www.techsoup.org and Idealware hosts a number of software comparisons www.idealware.org

8.3 Sources of advice

Advice is something you get to avoid you needing help at a later stage. Good technology advice is something that is available from Circuit Riders and other technology professionals. You can find a list of Circuit Riders who have signed up to a list of core working principles and more information about Circuit Riders at the UKRiders website <http://ukriders.lasa.org.uk>

In addition, Lasa maintain a list of individuals and suppliers that have proven track records of working with voluntary sector organisations who can help you – see the **Suppliers Directory** – www.suppliersdirectory.org.uk

8.4 Further resources and publications

Computanews – a quarterly technology magazine published by Lasa for small and medium sized voluntary sector organisations.

www.lasa.org.uk/publications/computanews/

8. Appendices

Computanews ICT guides - Lasa also publishes a range of short guides on data protection, project management, security, managing technology and circuit riders. www.lasa.org.uk/publications/computanews-guides/

ICT e-bulletin - the free monthly ICT e-bulletin compiled by Lasa and Superhighways is aimed at smaller voluntary and community organisations, managers, circuit riders and accidental techies and contains news, events, training and learning, funding and awards, resources, practical tips, tools and applications and opinion. www.lasa.org.uk/publications/london-ict-bulletin

ICT Hub publications (available to download from www.ictHub.org.uk):

- A guide to managing technology
- How to cost and fund technology
- An technology survival guide for trustees

Managing technology to meet your mission – A US publication from NTEN – Written by and for non-profit technology staff and non-profit leadership staff, this collection of case studies, analyses, and guidelines shows how technology can be strategically deployed in their organisations to better accomplish a nonprofits' mission. See www.meetyourmission.org/ - book available from Amazon.

Data Protection in the Voluntary Sector – third edition of Paul Ticher's standard work on the subject – available from The Directory of Social Change www.dsc.org.uk/Publications/Law/@54046

Wired For Good by Joni Podolsky - a nuts-and-bolts guide to strategic technology planning for non-profit organisations, available from Amazon.

Lasa is the trading name of Lasa Charity UK Limited, a registered charity in England and Wales. Charity Reg No: 800140. It is a private company limited by guarantee, registered in England and Wales. Registered office: Universal House 88-94 Wentworth Street, London E1 7SA. VAT No 524965032

London Councils is committed to fighting for more resources for London and getting the best possible deal for London's 33 councils. London Councils has a website about its grants service. To read about our grants funding and the work of some of the 300 groups we support please visit www.londoncouncils.gov.uk/grants