ICT Security

practical guidance for the voluntary and community sector

This guide aims to provide practical guidance for voluntary sector staff who have responsibility for managing and securing ICT systems.

Whilst it can't hope to cover every single aspect of ICT security, it provides an introduction to the risks to computer security and how you can avoid them.

ICT (Information and Communications Technology) is now integral to the way nearly all organisations work. We rely on computers to get our jobs done, and much, if not all of our important organisational information and data is now held on computers.

From a 2008 Lasa survey of ICT access and use in an inner London borough almost 90% of respondents said that computers and the Internet were "vital" or "fairly important". But respondents were also not planning for or managing ICT as:

- 55% lacked an ICT budget
- 65% didn't back-up data on a regular basis
- 51% didn't update anti-virus software on a regular basis

ICT equipment is often hard-won, particularly for smaller organisations so it's worth looking after! How long could you manage without your computers and related equipment? What would be the consequences if your organisation's important information (e.g. accounts or confidential client information) got lost or ended up in the wrong hands…? How would this affect your capacity to provide a service to clients and ability to respond to funders?

computanews security guide

is produced by Lasa

Editors:
Ian Runeckles & Aba Maison

Peer review:
Morgan Killick
Maher Al-Ugaily

Illustrations:
Phil Evans

Design:
Miles Maier

Universal House
88–94 Wentworth Street
London E1 7SA

Contact us:
020 7426 4473
computanews@lasa.org.uk
www.lasa.org.uk/publications/ict-publications/

About Lasa:
Lasa has been providing the voluntary and community sector with high quality and impartial ICT advice since 1984.

Subscribe

If you would like to subscribe to your own copy of **Computanews** and other Lasa publications such as the London ICT e-bulletin go to...

www.lasa.org.uk/lasa/mailing-lists/

contents

How to use this guide

ICT security is a large subject and to make it more approachable we have used a rating system on each section to help you:

Basic security

Every organisation should implement this, your organisation would be seriously at risk if you don't.

Enhanced security

All organisations regardless of size should consider taking the measures indicated.

Advanced

Particularly important for larger organisations with more complex systems or for those dealing with sensitive information especially where held on portable devices or media.

However, it is impossible to be completely prescriptive about security – only by carrying out a risk assessment as described in the first section of this Guide will you know how much detail to go into on any security issue.

At the end of most sections there are links to appropriate ICT Knowledgebase resources, with a list of general resources at the end of the guide.

If you have any comments or suggestions then we'd love to hear from you at the **Knowledgebase Discussion Forum** (*www.ictknowledgebase.org.uk/forums/index.php*).

ICT Security in context - A (fictional) cautionary tale…

Madeuptown Youth Action (MYA) is a small voluntary organisation working with youth in Madeuptown. The organisation has funding for a small project to produce web based information on other organisations in the region working with young people.

Pat recently joined MYA as a volunteer through Madeuptown Volunteer Bureau. He's given access to a the organisation's network so is able to use his computer to get onto the Internet and do some research, collate and publish the results on the organisation's website. He works hard and is popular with the staff and other volunteers.

On several occasions, Emily, a member of staff walks past Pat as he is working and sees him quickly switch to another program when he notices she is nearby. Curious that he appears to be hiding something, one day while Pat is away from his desk, Emily sneaks a peak at what Pat has been working on. To her horror, on firing up his web browser, Emily sees that Pat has been looking at porn sites and is extremely offended by what she sees. She also notices that in the background another program is downloading music.

Emily walks away not really sure what to do. After all, Pat might rightly feel aggrieved that she was poking around on his computer. She does feel really strongly however that Pat should not be engaging in this sort of activity by using the organisation's computers.

Not long afterwards, some of the organisation's computers are hit by a very nasty virus and Pat's computer in particular experienced a lot of issues. MYA call in their ICT support volunteer who spends several days trying to clean up the affected computers. Whilst the computers are being cleaned up, staff are unable to work on them so there is a lot of disruption and stress. Much of the material Pat has been working on also is lost as he has been saving to his computer which was badly affected by the virus.

The problem is eventually traced back to the computer Pat has been using. Pat had installed some peer to peer software so he could download music, all of which was copyrighted. It was also likely that some of the less desirable sites he was visiting had installed malware (software programs designed to infiltrate or damage a computer system without the owner's knowledge).

MYA does not have any policy about acceptable computer use, and because they rely solely on a volunteer with limited availability to support their computers, antivirus software and operating system updates are not always kept up to date.

Emily feels really bad that she did not raise the issue sooner as the situation might have been avoided. However, in the absence of any policies around computer use she felt she really didn't have a leg to stand on.

Perhaps if MYA had read this guide, they might have avoided a lot of problems…

Part 1 - Risk assessment and policies

Risk assessment

Many of the potential risks faced by organisations relate to information held in ICT systems (for example an organisation's accounts are likely to be held in a spreadsheet or accounting program on a computer).

Additionally, organisations are often required to meet requirements made by various governing bodies and stakeholders to carry out risk assessments. For example **The Charities (Accounts and Reports) Regulations 2000** (*www.opsi.gov.uk/si/si2005/20050572.htm*) mean that charities with a gross income of more than £250,000 have a legal requirement to include a risk management statement in their Annual Report (for more information see the Charities Commission guidance *www.charity-commission.gov.uk/investigations/charrisk.asp*).

Apart from the Charities Commission, other bodies, laws and regulations, quality frameworks etc. often require some element of risk assessment to be carried out, since information and data needs to be protected, and comply with regulations.

Whether or not there is a legal requirement to do so, doing risk assessments is good practice for any organisation that wants to carry on its function because without knowing what the risks are it's impossible to manage them.

Risk assessment steps

One of the first steps to tackling ICT security issues is to identify and assess the risks. The risk assessment process can be broken down into four main phases:

1. ***Identifying the risk***
   What can go wrong? (e.g. loss of accounts or financial records)

2. ***Evaluating the risk***
   How likely it is to occur and (e.g. high, medium, low likelihood)

3. ***Analysing the risk***
   What would be the consequences if the risk did occur (e.g. unable to produce or monitor finances and budget if accounting records lost)

4. ***Managing the risk***
   Once the risk factors have been established, organisations will need to put systems, policies and procedures in place to minimise the effects of the risk should it occur (e.g. daily back up of computerised accounts).

ICT risk includes the loss any ICT resource or system that would affect an organisation's ability to carry out its mission or function. Managing ICT risk needs to be included in an organisation's overall risk management strategy.

ICT risk will change as new technologies are adopted to support the organisation's mission. Since ICT is so fundamental to the way most organisations operate, there are several areas to consider such as...

The technology itself

This could be both hardware (the physical components) and software (the applications or programs run on a computer). Examples of risks include:

- The hardware or software fails to meet the organisation's operational needs (e.g. newly implemented network, database, finance package etc.)
- The equipment itself fails, or proves unreliable (e.g. old / obsolete equipment)

Carefully assessing and reviewing your ICT needs as part of your overall ICT strategy, drawing up appropriate requirements, carefully assessing suppliers, and properly managing ICT projects are ways of reducing these types of risk. In addition organisations should ensure that they have access to adequate and appropriate technical support for their technology.

Security of assets

This includes both the physical security of equipment, and protecting data held on computer systems. Risks include:

- Loss or damage (e.g. computer system failures such as network going down, or loss of data such as accounting information or important information held in a database, flood or fire damage)
- Theft (e.g. of computer equipment, data held on computers)
- Unauthorised access to information (e.g. internet) or equipment

Legal

Organisations need to consider the potential legal risks that could arise. This list is not exhaustive:

- ***Data Protection Act***
  (e.g. failing to adequately protect personally identifiable information, inappropriate marketing)
- ***Charities law and Companies Act***
  (e.g. financial reporting requirements not met because of computer systems going down and failure to do adequate backups)
- ***Disability Discrimination Act***
  (e.g. failure to provide suitable computer equipment to disabled employees, failure to make reasonable adjustments to make your website accessible)
- ***Health and Safety Act***
  (e.g. failure to provide suitable display screen equipment or working arrangements that allow computer users to take adequate breaks)
- ***Software licensing and copyright regulations***
  (e.g. using unlicensed software, employees downloading music onto work machines, using copyrighted material on your organisation's website without the permission of the copyright owner etc.)
- ***Breach of libel laws***
  (e.g. inappropriate use of Internet / email by staff such as libellous or defamatory material sent by email or posted to Internet sites)

Procedures and Policies

Procedures and policies are important in terms of managing risk, but in addition to this, an absence of them can expose organisations to various risks:

- Abuse of computer equipment or systems by staff or other users
- Inability to recover from "disaster" such as loss of important data held on computers

See the section on **Policy and Governance** in this guide for more information.

Of course merely having the procedures and policies in place is not enough. They will need to be enforced and regularly reviewed.

Who should carry out the risk assessment?

Again this will depend on the nature of your organisation however appropriate staff might include:

- ICT manager or other person responsible for the organisation's ICT (e.g. the "Accidental Techie")
- Office Manager
- Trustee or board member

The most important thing is that someone is identified and given the responsibility and that the risk assessment is planned for, carried out, and the results documented.

How often should we do a risk assessment?

Depending on the size and role of your organisation the amount of ICT risk you'll be exposed to will vary. This will impact on the frequency with which you need to carry out a risk assessment. However, for most organisations this should be done at least annually and when there is a significant change such as:

- Introduction of a new software system e.g. implementation of new accounts system, database
- Introduction of new hardware or major upgrade of existing hardware system (e.g. new network installation)
- A move to new premises
- Major refurbishment of existing premises
- Change in staffing (e.g. loss of key personnel)

Whatever the size of your organisation, it is important to properly assess what the risks are so you can act to minimise them.

How do we carry out an ICT risk assessment?

There are some useful tools to help you carry out a risk assessment including:

- Appendix 1 - Countering and Reducing ICT Security Risks
- Appendix 2 - ICT Risk Assessment Checklist
- Business Link ICT risk assessment tool *www.businesslink.gov.uk/bdotg/action/ITRiskAssessment?r.s=sl*

Knowledgebase

ICT Risk Assessment
www.ictknowledgebase.org.uk/riskassessment/

Securing Your Network – Major Threats And How To Avoid Them
www.ictknowledgebase.org.uk/securingnetwork/

Policy and governance

Who's responsible?

Decisions on your ICT policy, together with decisions on any aspect of ICT which will have a major effect on the way the organisation works (such as security) must be taken at Board or Management Committee level. Whether the members like it or not, it is just as much a part of their responsibility to take sound decisions about ICT as it is about finance or the appointment of key staff.

Once policies have been put in place, or a broad strategy has been established, many routine decisions can be taken by staff, without reference back to the Management Committee. It is important, however, that decisions are taken within the framework of the organisation's policies and overall goals. This means that the decision or recommendation often needs to be checked by the manager or someone who is aware of the wider strategic issues - again whether they feel technically competent or not.

Finally, there is a level of day to day management of ICT which is appropriate to be delegated. Even here, it is essential that the person doing the ICT management not be given carte blanche; they should be given clear targets and guidelines, drawn from the policies.

For more general information on the responsibilities of voluntary sector management committees and boards see the **ICT Hub publication From Nightmare to Nirvana - an ICT survival guide for trustees** (see Resources/Further Information)

AUP structure

Introduction
- Who does this policy apply to?
- Why have an acceptable use policy?
- How is it published & communicated to users?
- Disciplinary procedure

General computer use
- Usage
- Software installation
- File management
- Fault reporting/support
- Disaster planning

Email
- Work-related use
- Personal use
- Anti-social or unacceptable usage
- Signature files
- Attachments (sending & receiving)
- Viruses
- Mailbox management
- Mailing lists
- Spamming

Web & other online uses
- Work related use
- Personal use
- Downloading
- Offensive material
- Messaging/chat
- Online purchasing

Security
- General security requirements
- Data Protection
- Passwords
- Back Ups
- Internet
- Anti-virus
- Network administration
- File management

Training
- Induction
- Needs analysis

Acceptable Use Policy

An Acceptable Use Policy (AUP) provides ground rules to users of the organisation's ICT resources be they staff, volunteers, clients, trainees, management committee, or trustees for acceptable use of the equipment etc. so there are no misunderstandings. It should also provide guidelines if, for example, misuse occurs. An AUP also demonstrates to potential funders that the organisation is professional in its approach to managing users.

Framework for policies

Lasa's Acceptable Use Policy Framework Document (see Knowledgebase links below) contains suggested headings and topics which will be applicable for a typical AUP for a small voluntary sector organisation.

The framework has attempted to cover most of the areas which will be required for an AUP but not all need be adopted e.g. if an organisation only has a small number of standalone PCs then the specific items on networks etc. will not be necessary.

Of course, should the organisation change its ICT infrastructure then the AUP will need to be revised - we suggest that the AUP is reviewed every year as new technologies etc. will have impacted upon it.

AUP implementation process

The following is a suggested process for initiating and implementing an AUP - this will differ depending on the size and nature of the organisation.

AUP process

1. Initiate - discuss in team/staff/volunteer/management committee meetings etc.
2. Form a working group (if appropriate) to draw up AUP
3. Use framework for consultation with users and gain feedback
4. Draft policy and circulate amongst working group for comment
5. Write up final policy
6. Publish and distribute
7. Publicise to people in organisation
8. Monitor and review annually

Knowledgebase

ICT Acceptable Use Policies
www.ictknowledgebase.org.uk/acceptableusepolicy/

Data protection

The **Data Protection Act 1998** regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act. The Act applies to personal data - information about identifiable living individuals that is:

- Held on computer or any other automated system
- Held in a relevant filing system (a paper system such as client records system, or a set of files on service users that is organized alphabetically by the name of the person or some other identifier such as case number)
- Intended to go onto computer or into a relevant filing system

The Data Protection Act applies mainly to the Data Controller - the person who decides why and how personal data is processed. This "person" doesn't have to be an individual and in most cases will be an organisation. Individual members of staff or volunteers will merely be agents of the data controller.

The Act has eight Data Protection Principles that cover issues including the processing, accuracy, security and lawfulness of data collection as well as the rights of the Data Subject.

For the purposes of this guide we are examining only the **seventh Data Protection Principle** which says that you must have "appropriate" security to prevent two kinds of problem:

- unauthorised access
- accidental loss or damage

The use of the word "appropriate" here relates directly to the aim of preventing harm. You need to carry out a risk assessment to see how much harm, and to how many people, would result from a breach of security, then put your main effort into preventing the most serious harm.

Before looking at security you must spell out what access is authorised. Any other access is therefore "unauthorised". Some material could be in the public domain, with no restriction on access; for this, obviously, no security might be needed. For more confidential material it is important to be clear where the boundaries of confidentiality lie: will the information a client gives you stay just with the case worker? or with the case worker and their supervisor or their team? Or within the organisation?

And despite all that, under what circumstances would you breach confidentiality in order to protect other people? Everyone benefits from this clarity: your staff and volunteers, your clients, your funders and other external agencies that you come into contact with.

Having decided who is allowed to see the information, and in what circumstances, you then must ensure that you prevent other people from seeing it. The measures you take must be "technical and organisational". Technical measures would include physical security – locks and barriers to access – and things like passwords, anti-virus software and back-up systems. Organisational measures are usually more important: training (and policies to base training on), induction, supervision and a general culture of security.

You should also think about the always thorny issue of how to encourage people to spot and own up to security breaches. Inevitably things will go wrong; the best organisations learn from their mistakes, and offer redress without being forced into it. But security breaches are usually embarrassing so the natural tendency is to hope that no one will notice.

There is a British Standard on **Information Security Management** (BS7799, also known as ISO 17799). While this has some useful pointers, it is more appropriate for very large organisations which need more formal systems and can afford the cost of being assessed for compliance regularly.

Knowledgebase

Make Sure Your Data Protection Compliance Is In Order
www.ictknowledgebase.org.uk/dataprotectioncompliance/

Data Protection Policies
www.ictknowledgebase.org.uk/dataprotectionpolicies/

The Lasa Computanews Guide on Data Protection. (209 kb PDF document - requires Adobe Reader)
http://bit.ly/1qCkim

Inventorying and licensing

Organisations need to know what equipment they own for various purposes – support companies will often want to know before quoting for annual costs; the auditors will want to see an asset register which is required for annual accounting; insurance companies when putting a policy together. Inventorying your hardware and software can be done manually (using a template, and keeping a paper copy handy) or by using automated methods such as **Belarc Adviser** (*www.belarc.com*) or **SpiceWorks** (*www.spiceworks.com*).

For hardware is useful to record (if appropriate):

- Organisational ID
- Manufacturer
- Model
- Serial number
- Asset tag
- Processor and speed
- Hard drive capacity, RAM
- Operating system
- Upgrades
- Purchase date, supplier, invoice reference and price
- Warranty information

For software:

- Name, manufacturer
- Version
- Purchase date, supplier, invoice reference and price
- License key

It is also important to record other settings and passwords, for example:

- Routers, firewalls, wireless access point
- Websites (administering, ftp)
- Servers
- Hosted services (for example, web filtering, spam/virus filtering, Flickr, YouTube)
- Internet account

To help with this a new ICT handbook has been conceived, and as it is a supported, low-cost, low-tech paper-based solution, it is simple to use and accessible by anyone in the organisation. The handbook will come in two flavours - **WEknow IT**, aimed at supported organisations and **MYknow IT**, a free PDF download for unsupported small organisations. It will be available as a download from *www.knowit.org.uk*

Software licensing misuse

If you are in charge of keeping track of your organisation's technology, you know that software presents you with a unique set of problems. Unlike hardware, software is hard to pin down. Software licenses tend to be written for a legal audience, and even to lawyers, they may not be particularly clear. However, understanding software licensing is crucial to managing technology within your organisation.

In brief, proprietary software (which costs money) cannot be redistributed or modified and you purchase a license to install it for each machine e.g. Microsoft Office. Some software is available to be purchased at charity discounted prices or through donation schemes such as that operated by **CTX** (*www.ctxchange.org*)

If you are using proprietary software which requires a license, then you'll need to keep track of it. Applications such as SpiceWorks mentioned above tell you how many installations of a particular piece of software you have.

Knowledgebase

Sample ICT Inventory
www.ictknowledgebase.org.uk/sampleinventory/

Making Sense of Software Licensing
www.ictknowledgebase.org.uk/softwarelicensing/

A Guide To Microsoft Licensing
www.ictknowledgebase.org.uk/microsoftlicensing/

Insurance

All ICT equipment should be insured against the usual risks – fire, theft, flood and so on. Usually this can be arranged through a normal office contents policy and is the cheapest option. However, you'll need to be sure that equipment that is portable such as laptops is insured for out of the office. Watch the small print to see if you will get "new for old" – computer equipment depreciates quickly so you might not get much back.

Also ensure that equipment that is not normally on site, perhaps at a staff member's house for home working, is also insured or that it has been arranged through their own home insurance policy. Don't forget to keep the inventory up to date so this can be sent to insurers when obtaining quotes or updating the register of insured equipment.

Standards – ISO/IEC 27001

ISO/IEC 27001 is an international standard which defines the requirements for an **Information Security Management System (ISMS)**. It is designed to ensure the selection of appropriate security controls for an organisation, large or small, although it is likely that only larger VCS organisations will be able to afford the resources to implement the standard fully.

The standard helps to protect information assets and give confidence to interested parties, especially clients and funders. The standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving your ISMS.

Certifying your ISMS against ISO/IEC 27001 can bring the following benefits to your organisation:

- Demonstrates the independent assurance of internal controls and meets governance and business continuity requirements
- Independently demonstrates that applicable laws and regulations are observed
- Independently verifies that risks are properly identified, assessed and managed, while formalizing information security processes, procedures and documentation
- Proves your trustees and management's commitment to the security of its information

More information about the Standard can be found at *www.bsi-global.com*

Part 2 - Security and computer use

People security

People can be the biggest threat to the security of your ICT systems whether inadvertently or deliberately. No matter how technically secure your ICT systems are, people can often be your weakest link.

It is important that staff are educated about the potential risks and how to avoid them. For example, your organisation may carefully enforce secure and regular password changes to access the network itself. However, if staff then write down their passwords on a sticky note stuck to their monitor, anyone who has physical access to the computer will be able to gain access to the computer and your network with potentially serious or embarrassing consequences.

It is also possible that staff could be tricked into revealing important passwords to convincing "confidence tricksters" either by phone or email. Treat any requests to give out a password with extreme suspicion. Is that phone call claiming to be from your ICT support company and wanting the password for your server genuine? Is that email requesting you click on a link to update your login genuine? Almost certainly not! Your ICT support company probably already knows your server password, and if your login details really need updating you're highly unlikely to be notified of this by email.

Make sure you avoid storing sensitive data unencrypted on portable media such as memory sticks, CDs, DVDs etc. as these can be easily lost.

You should also ensure that you disable network accounts for staff who have left the organisation. This is especially important if you have remote access to email or files and the staff member has left 'under a cloud'… Changing passwords regularly will also assist with this – see the section on **Passwords.**

It's also a good idea to make sure you know who has access to your systems and data, and that they are authorised to do so.

Physical security

Physical security of ICT systems is something that can easily be overlooked with often disastrous, expensive, or embarrassing consequences (or all three!). Even if you have insurance you will recover the cost of buying a new server or a PC but the data and configurations in the stolen kit is more valuable than the replacement cost.

General precautions

Since buying your ICT equipment is one of the most expensive capital investments you'll make, taking a few sensible precautions will reduce the risks affecting your organisation:

- Consult your local police for advice on securing entry points to your office, burglar alarms etc.
- Insure your equipment - most office contents policies will cover PCs - but check to make sure your policy does (see section on **Insurance**)
- Keep a register of equipment (see section on Inventorying). Keep a paper copy in a fireproof safe and offsite - don't rely on just having it electronically – and keep it up to date
- Keep copies of essential software in a safe or off site along with the license keys (the set of numbers and/or letters which you are asked for when you install the product) provided by the manufacturer
- Mark equipment with approved anti-theft markers and investigate physical locking devices
- Buying new equipment? - don't leave the boxes on public display outside!
- Have a disaster recovery plan in place - find out how you could get hold of replacement PCs and a server fast

How long will the estimated down time for the organisation and the estimated buffer time for the organisation to be able to function after disaster? You can download **nPower's Communications, Protection, Readiness guide** to business continuity and disaster recovery at *http://npower.org/files/page/CPR.pdf*

Building access

Opportunist thieves abound, don't make it easy for them. This applies to all organisations and is particularly important where your building or office is readily accessible to the public, or where open windows are accessible from the street.

Make sure you know who has access to your building or office(s) and take appropriate measures. For example:

- Lock valuable items such as laptops, data projectors etc. away, store keys securely and make sure only authorised people have access to them
- Escort and supervise all visitors and if necessary have them sign in / out
- Change any door codes regularly
- Use a security alarm and make sure it is set overnight or during other long periods when the office will be unattended
- Ensure office keys are handed back when staff leave the organisation

Extra precautions for ICT equipment in public areas of your building or office

Public areas are notorious for the ease in which equipment can "go missing". In addition to having up-to-date inventories, adequate insurance and indelible security marking, PCs and monitors should be secured either to the desk on which they sit or an adjacent wall using an appropriate device which doesn't damage the casing such as a cable lock. Your local supplier may have such devices, otherwise check out specialist suppliers such as **PC Guardian** (*www.pcguardian.com/guide.html*). You could also consider housing the PC workstation in a lockable cupboard.

If you are running an outreach service or mobile training suite using laptops then the same principles apply only more so.

Knowledgebase

Giving Your Service Users Access To Your Computers
www.ictknowledgebase.org.uk/publicaccesstoyournetwork/

Mobile security

With the advent of wireless technology and convergence of devices, use of computers on the move is now widespread. Whether on a laptop, PDA (personal digital assistants – hand held computers) or smart phones (mobile phone with advanced, often PC like functionality), it is easy to take your work with you and this presents increased risks to the security of your organisation's data.

Loss and theft

A big risk with highly portable (and desirable) devices is loss and theft. As well as taking precautions to avoid these mishaps, it's worth preparing for the event that the worst should occur.

At the very least, ensure that devices are protected with a strong password. Consider carefully whether sensitive data needs to be present on mobile devices at all. Where it is absolutely necessary, make sure it is encrypted so it cannot be read by unauthorised persons.

Some good practice tips for physical security would include:

- Make sure your equipment insurance also covers laptops and other portable devices when they are off the premises
- Lock laptops away at night or when the office is unattended
- In transit - don't leave in full view whilst in unattended cars
- Case study - laptop carry cases are easily identifiable by thieves so consider carrying them in something not as obvious
- Home use - remind staff that the equipment is for work use and not for running dodgy games they bought at a car boot sale.

Also, if household members use the computer, ensure sensitive files aren't accessible.

Using your laptop in public places

In addition to loss and theft, remember that in public places you can easily be overlooked (commonly known as "shoulder surfing") so it might not be a good idea to type that very private letter on your laptop whilst eating your morning croissant at the local coffee emporium. You'll also want to make sure you shield your password and be extra careful not to leave your laptop or other device unattended.

If you are using your laptop to connect to the internet in a public space such as a coffee shop or hotel lobby, or other free "Wi-Fi Hotspot" remember that these types of wireless network are inherently not very secure. This is because in order to make it easy for users to get onto the network, wireless security measures are often not implemented.

Wireless networking presents security challenges, which we discuss later in this guide.

Using public access computers

The availability of public access computers (e.g. in Libraries, Internet Cafes, UK online centres etc.) is another modern day convenience. For some very small organisations that don't have their own equipment, public access computers are a necessity not just a mere convenience. See box in next column for safer use of public computers.

Knowledgebase

Giving Your Service Users Access To Your Computers
www.ictknowledgebase.org.uk/publicaccesstoyournetwork/

Precautions to take when using public computers include:

- Take extra care when accessing your network remotely from public computers - who knows whether some key logging software has found its way onto a machine, giving someone else all the information they need to log onto your network
- Make sure that passwords and other login details are not being saved automatically when you are online. Many browsers and websites offer this option but on shared computers make sure the "remember my ID on this computer" is NOT ticked
- Clear the browser's internet cache and any other personal data such as form data and passwords when you have finished your session
- Never leave the computer unattended when you are logged in
- Watch out for people looking over your shoulder when entering passwords;
- Make sure you sign out of any websites and computers completely. It is important that you do this even if you have not requested the computer remember your login details
- Avoid using shared computers for logging into websites that hold your personal financial information

Homeworking and Remote access

Your organisation is responsible for the data processed by your staff, regardless of where they do it. The main difference between working in the office and out of it is in security. What would be the consequences if your staff lost crucial data between home and the office?

You may decide that emailing documents to and fro, or giving staff direct access from home to their documents at the office is less of a risk than sticking files onto USB memory sticks or giving people a laptop which could get stolen en route. How much would it matter if your worker's partner or teenage children accessed confidential documents on the computer at home? Should you insist on a separate computer for work and home use? Should you provide specific equipment, and insist that it only be used for work? How are you going to support it? Will your current ICT support company carry out home visits if necessary? Or is it enough to ask people to use passwords on their documents and to keep their work in a separate area of the computer?

Some good practice pointers:

- Allow home working with the backing of management, rather than letting it grow on an ad hoc basis
- Whilst remote access is convenient, the solution itself should be set up securely and staff must be security conscious at all times
- Create a security policy and educate remote workers on how it affects them
- If you provide equipment for home, ensure it is used for work purposes only and should

not allow friends or family members to use it
- If using virtual private networks (VPNs) ensure adequate levels of authentication and passwording – perhaps use a dedicated SSL box
- Consider thin-client applications (e.g. Terminal Services, Citrix, VMWare) for remote workers so that data is never stored locally. In this situation, the homeworker runs a session on their computer over a broadband connection which gives them a desktop which is stored on a dedicated server and provides access to files and network services exactly the same as if they were on a PC in the office
- Monitor the status of all computers, and check virus updates regularly for remote workers
- Advise on the use of personal firewalls
- Insist on shredders in the home to prevent information being stolen
- Don't make security too restrictive so that remote workers work around it
- Create a support policy so that remote workers know when they can access support - people tend to work more flexibly at home without the time restrictions of an office being open
- Remote users shouldn't leave their home PC unattended and logged in to the office network
- Ensure that remote users can't install software on the office network

Knowledgebase

Home Sweet Home? The Joy of Telecommuting
www.ictknowledgebase.org.uk/telecommuting/

Part 3 - Securing your ICT assets

Passwords

Computer systems generally use a username/password combination – the username tells the computer who you are, and the password is the shared secret that only you and the computer system both know. By giving both, you gain access to the parts of the system you have been permitted to use.

Many people think of passwords as just another hoop to jump through - something you have to remember to do but has no real intrinsic value. Yet in many cases, passwords may be the ONLY defence against the hacker and deserve to be taken seriously no matter how low the risk is.

If someone else discovers your password and username, they can access the computer system and do anything you could to it, all in your name. More sophisticated brute force attacks, called dictionary attacks, use lists of words that are commonly used in passwords rather than changing one character at a time. These lists might include every word in the English dictionary or a foreign language, meaning even rare words are not as secure as you might think.

If you operate a peer-to-peer network, a single password to gain access to a PC may unlock all of the shared documents on your network as well as your personal files. In a server environment, network administrators centrally control passwords including enforcing minimum length, complexity and frequency of changing passwords. Don't give out the administrator's password to staff who don't need it. Your support contractor will need to know it though.

Password policy

It is important to have a password policy - ensure that passwords for logging on to the system are not obvious, aren't written on post-it notes attached to the monitor, and are changed at regular intervals. Staff should not divulge their passwords to other members of staff (including the administrator) – in some commercial organisations this is a breach of policy and rewarded with the sack.

Whilst this might be a little too harsh for most voluntary sector organisations, if there is a need to allow staff to have access to email or files during staff absence this can usually be done through making changes on the server.

Use a password protected screensaver if you are working in a public area - alternatively ensure publicly accessible PCs cannot access important data.

Knowledgebase

How Am I Supposed To Remember That? Choosing And Using Secure Passwords
www.ictknowledgebase.org.uk/choosingpasswords/

Permissions

With a server based network, the level of security is racked up considerably over peer-to-peer networks (where files are stored either on individual machines or on a shared machine). A server provides a much higher level of security as to who can access the folders through the application of file permissions. The server administrator needs to apply the permissions – training is necessary for someone new to server admin.

The staff team will need to decide who has access to which folders. This is, of course, not set in stone, staff can be added and removed as necessary but it helps to have some sort of plan. For example, the finance worker and the director probably both need access to the Finance folder, but only the director to the Personnel files. If there's a management team then they can share certain folders that only they need access to and so on.

Choosing a password

Use strong passwords - avoid dictionary words, use a mixture of at least 8 letters and numbers and possibly mix cases especially for the administrator password - but don't forget it! User passwords are easy to change by your administrator - admin. passwords for server access are not easily recoverable. This may be enforceable through the server configuration. Make users change passwords on a regular basis, perhaps every 3 months – again this can be configured on the server where a warning is given in advance.

Remember that it is not just a question of confidentiality, but also of security – if an inexperienced user wanders into an area where they shouldn't be and accidentally deletes files it could be problematic. Security protects you against this as much as it does against malicious hackers - who in reality are much less likely to be wandering around your network. Folder names are visible to anyone with access to the server but they won't be able to open or save documents to the folder unless they have the relevant permissions. Folders or sub folders can be made read only to certain users so that changes to documents cannot be made – for example, you may want staff to be able to see the staff handbook information but not be able to alter it.

It is good practice to set up a few virtual or mapped drives – your network contractor who's setting up the sever can do this for you. On a server you might have three mapped folders - letters allocated here are arbitrary:

- G: Company – where the organisation stores all its work files (finance, personnel, projects etc.)
- S: Shared – templates, forms, resources, staff handbook, temporary files such as Antivirus updates etc.
- U: Users – personal documents (each staff user has their own specific folder which can only be seen by them)

Countering viruses and spyware

One of the best ways to bypass security is to trick the user into providing information direct to the hacker. In order to mitigate this type of risk, network administrators need to be certain that all of their users are aware of phenomena such as phishing and do not give information out by responding to hoax emails or telephone calls. Similarly, incorporating confidentiality into company handbooks and Human Resources/Employment Policies is a must.

The inexperienced (or irresponsible) user can also create havoc on a network by visiting high risk websites such as those concerned with shopping, MP3's, 'smileys', gambling, dating, chat rooms, pornography, free software, peer-to-peer file sharing etc. At first this may seem trivial but can expose the network to far more serious risks. The 'cure' for these risks, is to have regularly updated anti-virus software installed and scanning on all machines as well as specialist anti-spyware / pop-up blocking tools where needed. On the preventative side, you will need to ensure that all updates for the operating systems and web browser software are downloaded and installed.

If you operate public access PCs, you should consider options for governing the websites that users can access. Web content can be controlled on a network either through an advanced firewall or through a proxy server. Both systems regulate all requests for web pages and allow administrators to decide whether access to a particular website or type of website is permissible or not. This will usually involve some form of subscription-based service that actively monitors and categorises web pages.

Unlike spyware, pop-ups and

trojans, viruses target users indiscriminately. Smaller organisations are particularly prone to viruses as those using its computer systems often don't think about security.

Nevertheless, regularly updated and valid virus protection should be considered essential for every PC (especially Windows PCs). Installation is however different from installing on a single PC and you should seek professional help where needed.

If you are responsible for a network, look for specialised virus protection than can be centrally managed and monitored. In this way you can ensure that updates and scans are not being cancelled ,and you can keep track of threats - and even remove them without disrupting users.

These can usually be obtained from charity software suppliers at discounted rates.

Knowledgebase

Dealing With Viruses
www.ictknowledgebase.org.uk/viruses/

Choosing An Anti-Virus Solution For Your Organisation
www.ictknowledgebase.org.uk/choosingantivirus/

Firewalls and proxies

Automated – and therefore random - 'probing' of computers connected to the internet is a fact of modern life. Even those running a low risk environment will need a basic router with some firewall capabilities to ensure that these probes do not yield results – usually referred to as NAT (Network Address Translation). Such routers may come as part of your broadband package along with wireless access. Entry level broadband routers have some basic firewall and content filtering settings that could be enabled and set up to reduce risks and to support the organisation's AUP.

Clearly, the higher the risk, the more sophisticated the firewall needs to be. Whilst a router will usually suffice for a medium risk SOHO environment, if you run a higher risk environment you may need to consider something with more advanced features that can fend off sustained and deliberate attacks. Before you buy, be sure you understand what these firewalls do – they are unlikely to prevent viruses or spyware. Don't forget to change the default password on the router too – the manual will tell you how.

A firewall is a system or group of systems that enforces an access or deny policy that is set up by default but can then be configured to your own needs. The firewall filters all the packets of data that go in and out of a network and blocks them or allows them to continue to their destination. For example, you can configure a firewall to allow only email to enter your network, thus shielding you from any attacks except for ones via email. Note that a firewall is not a substitute for good anti-virus software, regularly updated.

A firewall often includes or works alongside a proxy server. A proxy server is a computer that also sits between computers on an organisation's network and the Internet. It allows an organisation to ensure security and administrative control (amongst other things). This way information on your organisation's network can be hidden from the outside world. A firewall also acts as the concentrator for your Internet access. Since all of your traffic goes through one place, you can produce great logs of who tried to access your network, what traffic went where, and much, much more.

Firewalls can be software or hardware-based. Recent operating systems (such as Windows XP, Vista, Mac OSX and Ubuntu) include firewall software which is adequate for most situations but can interfere with some network services and may be disabled for this reason in an organisational situation.

It is common in larger organisations not to rely on their router but to have a dedicated hardware firewall which may also have other uses such as controlling remote access to resources via a VPN (Virtual Private Network) over the Internet. These are not expensive nowadays - a competent firewall may only be the size of a paperback book but will be powerful enough to handle many users.

There are open source firewalls such as **SmoothWall** which can be installed on a redundant desktop PC but will require a competent techie in the organisation or support company to configure and support it.

As with other hardware the firewall needs to be kept updated. Manufacturers will update the firmware and so a maintenance contract may be required.

Knowledgebase

Firewalls
www.ictknowledgebase.org.uk/firewalls

Backups

Why it is important to back up your data

You should have backup copies of all your data for a number of reasons - a file can be accidentally (or maliciously) erased, hard drives and other hardware can fail, your PC or server could be stolen, and, in extreme cases, disasters such as fire or flood can occur. This could mean losing all your data and information, which may be critical for the running of your organisation - how long could your organisation survive if it lost all its client data?

Organisations need to develop a good backup strategy which should be affordable, robust, easy to carry out, and tailored to the needs of the organisation.

Start the planning process by developing a written backup plan that tells you:

- What is backed up
- Where it is being backed up to
- Who is in charge of performing backups and verification
- When backup will be run
- Which software will be used to manage the backup process
- When a test restore will be done (a backup is no use if when you need it you can't restore back from it – tapes can corrupt, hard drives can crash and CDs and DVDs can rot)

Share the responsibility for backing up by getting this strategy approved by management.

What to backup and how often

The first stage is to take a broad look at the data your organisation holds, and sort it into three categories:

- High priority – databases, financial data such as accounts, email, current projects. This kind of data changes frequently as it is worked on day to day
- Archive for the long-term – closed projects, images, video. This kind of data changes very rarely – it usually represents finished work
- Compliance – data retention. Some parts of this data will change frequently, others less frequently

Don't be tempted to skip this step. You will regret it as backing up every category of data on a daily basis can be extremely costly and time-consuming, so it's important to identify how often your various data changes. For the average organisation, the percentage of data that changes daily is somewhere between 2% and 5%.

High priority data

Ask yourself if your organisation could cope if details of contracts with funders, monitoring returns, mailing lists, financial records, payroll and other crucial company information were wiped out. The answer is probably no - once lost these documents are almost impossible to replace or rebuild. Where possible, these should be backed-up on a daily basis.

You may also have to do some housekeeping to organise work on current projects into folders that can be easily located and backed-up.

Don't forget to backup your email - this provides a valuable record of work on current and future projects. If you have a web-based POP3 email service with your Internet Service Provider (ISP), don't rely on them to backup for you.

Many ISPs offer POP3 email accounts with limited storage space and will delete emails older than 30 days to make space for incoming email.

A safer alternative is to download a copy of your messages to your computer using an email client such as Outlook, Thunderbird or Eudora. Although each client has a different backup protocol, email files should ideally be backed-up on a daily basis.

Archive for the long-term

Archiving data from old projects is good practice as it allows you to safely store old files from closed projects and free up disk space.

You probably also have lots of images from events run by your organisation. If you don't use these files very often, they could be archived to DVD or external hard drive for safe-keeping. These files also tend to be quite large and slow down the daily backup.

You may also want to archive emails from closed projects as they still count as part of the historical record. Most email programs will allow you to archive old mail or create archive folders and drag mail into it before exporting.

Compliance

The laws concerning compliance with data retention are fast moving and constantly evolving. A good first step is to visit the website of the Information Commissioner.

The Information Commissioner. enforces compliance with the:

- Freedom of Information Act 2000
- Data Protection Act 1998
- Privacy and Electronic Communications Regulations 2003
- Environmental Information Regulations 2005

Secondly, review the data retention period that many funders set out in their terms and conditions of grant. A general rule of thumb is that financial and legal information should be retained for at least 6 years.

What to use

There are several methods you can use to back up your data. These include:

- CD/DVD-Recordable
- External hard drives
- Networked Attached Storage
- Tape
- Online back up services

CD/DVD-Recordable

Whilst in the recent past, floppy disks and other removable media such as zip drives were adequate to back up, they have little capacity and are generally outmoded.

Some organisations use memory sticks which although are cheap and convenient are a massive security risk – they are easily lost, broken (stick one inside your back pocket and sit on it…) or end up in washing machines. CDs have a capacity of 700Mb and DVDs 4.7 Gb (about six CDs worth) so unless you only have a very small amount of data to back up DVD should be used.

DVDs are universally available and relatively cheap. DVD-RW discs will allow rewriting but given the cost difference, they aren't recommended. DVDs can be damaged though which could be disastrous when trying to restore lost data – we'd recommend that an external hard drive is now a better option given the low prices.

External hard drive

These devices have become more popular as prices have fallen, and for good reason - they are mobile, fast, have large capacities, are portable and compact - all these things make them good candidates for backing up. Units are available which are tailor-made for backing up with capacities of up to 2Tb (2000Gb) and include basic backup

software. However, the fact that they are so mobile increases the risk of theft so a level of encryption will enhance security should someone try to get the data off them.

They could probably be used in conjunction with another method of backing up such as using DVDs or online as it's unlikely that you would want to regularly take the drive off the premises for disaster recovery purposes – a better alternative is to have a number of hard drives so one can be taken off-site.

Network Attached Storage

Another option is to use a NAS (Network Attached Storage) device as a primary backup device. Whilst they are bulky and would not then be removable they do have the advantage of being quick and in some cases come with multiple disc in a RAID formation so that there is built in redundancy (if one disc fails, the other will take over with no loss of data as in a server disc array).

There are also variations on the NAS which provide almost instant backup capability – there is no backup schedule as such (most backups are run overnight so files aren't being changed as the back up is being carried out and cause corruption) but files are backed up constantly.

Tape

Tape is still a common backup media - with appropriate software it's easy to use, the medium is small and portable so taking off site for security and peace of mind is relatively simple, it can store large amounts of data and tape drives are usually very reliable.

There are, bewilderingly, several different types of tape which have varying storage capacities - **DLT** is probably the most common for smaller organisations (up to 160Gb storage) with **SDLT** (up to 320Gb) and **LTO** (up to 1600Gb) catering for larger servers. Note that the tape drive needs to be matched to the capacity and type of tape you want to use - when selecting a drive, it's worth overestimating the amount of data you're going to back up - it's sure to increase! Capacity is given in the format 80/160 which means that this particular tape can store up to 80Gb uncompressed or 160Gb compressed.

You would generally only install one tape drive in a small organisation usually on the server or the main PC where you are storing information if you have a well structured peer-to-peer network. Make sure you do a test restore at least every quarter to verify and validate the backup sets

Online back up services

These take advantage of the popularity and availability of broadband connections to upload files to a web server. Many companies offer this service:

- **IBackup**
  www.ibackup.com
- **Back2go**
  www.back2go.com
- **Iron Mountain**
  www.ironmountain.com/digital
- **FlashBackup**
  www.flashbackup.com
- **Backupdirect**
  www.backupdirect.net
- **Ampheon**
  www.ampheon.co.uk
- **Zen backup**
  www.zen.co.uk

Your support contractor may have a favoured solution, so talk to them first before signing up. These services use incremental backups so that only the first backup would be of all the user files in the shared directories - after that it would only backup those files which were new or had been changed.

Software is provided allowing you to schedule backups out of office hours and to restore. This type of system is currently quite expensive unless you have small amounts of data to backup.

Backup software

Devices such as a tape drive or external hard drive can copy the entire contents of a hard drive automatically when you aren't around depending on the type of software you buy, for example, ArcServe, Symantec Back Up Exec and Dantz Retrospect.

Alternatively, if you have a Windows server (or PC), it comes with NT BackUp (Windows Backup and Restore Centre in Vista, Windows Server BackUp in Windows Server 2008) which can be augmented with BackUp Assist for more advanced backing up of, for example, Exchange mail stores.

Knowledgebase

Online Backup Services
www.ictknowledgebase.org.uk/onlinebackup/

Developing A Backup Strategy
www.ictknowledgebase.org.uk/backupstrategy/

Wireless

All flavours of the **802.11** (WiFi) standard are susceptible to a number of security vulnerabilities. As wireless networks use radio waves, anyone with the right equipment and know-how could tap into your network from outside your building (or from another office within a shared building). It is possible to encrypt data travelling across a wireless network using a technology called **Wired Equivalent Privacy (WEP)**. However this and other security settings are often disabled by default on wireless equipment. Added to this, WEP itself is not completely secure. Look out for newer products which use a system called **WiFi Protected Access (WPA)**. WPA promises much improved security over WEP.

However, it is possible to undermine the added security afforded by WPA if it is not set up correctly. For example, it is important to use a good choice of password and security keys to reduce this possibility. It is possible to upgrade some current wireless Network Cards to incorporate WPA - see your manufacturer's site for details.

WEP and WPA may provide adequate security for home wireless networks when used in conjunction with other security measures. For office wireless networks, additional measures will need to be taken to ensure security. Virtual Private Network (VPN) technology used in conjunction with wireless networking may provide a solution. In addition to the other network security precautions, there are others that should be taken to prevent casual access to a wireless LAN include:

- Enable Wired Equivalent Privacy (WEP) at the highest setting - whilst this does not guarantee security it's worth having
- Use WPA if available in preference to WEP
- Set up access points to allow access to known network cards only (each network card can be identified by a number called a MAC address) which combined with WPA2 (AES) is the most secure type at present
- Change the default SSID (Service Set ID or network name) and encryption keys (and don't use your organisation name). The SSID is the name by which an access point indentifies itself. Using the default SSID suggests to hackers that the rest of your setup is default, making your network a likely candidate for intrusion attempts
- Turn off broadcasting of the SSID. This makes it much harder for people to find your network, but you must tell your users what the SSID is so they can connect
- Put your wireless access point in the middle of the building, to minimise leakage outside

Knowledgebase

Virtual Private Networks
www.ictknowledgebase.org.uk/vpn/

Wireless Networking Security Considerations
www.ictknowledgebase.org.uk/wirelesssecurity/

Software updates

It is vitally important that software is kept up to date by installing security patches as they are released. All responsible software creators will release "patches" as

security holes are found in order to keep the threats at bay. There are a number of ways in keeping client server networks up to date.

If you are running a Windows-based network then the easiest way is by using **Windows Server Update Services** (WSUS). This gives administrators control over what patches to install and when – important when there are server patches to install which requires a server restart that this happens out of office hours and avoiding times when the backup is running.

It will also roll out updates to the client machines for all Microsoft packages. Macs and Linux PCs also have automatic updating services.

In addition to WSUS, there is dedicated proprietary software which can identify possible vulnerabilities to the network and make life easier in managing updates. For example, GFI LANguard will scan the network and when the scan is complete, it allows administrators to deploy and manage patches and security updates on all machines across the network. Hardware information can be retrieved and baseline comparisons used to check for unauthorised changes.

Peer-to-peer networks are harder to control but operating systems can usually be set to automatically download and install updates as they are available.

Web threats

Although it is still very important to install and keep anti-virus software updated, the tendancy to move to web 2.0 and hosted services means that threats to the organisation are more likely to originate from the web.

Malware and spyware can be filtered by using add-ons to anti-virus packages and are updated in the same way. It is also worth installing OpenDNS (see **Network Misuse** below)

Knowledgebase

Removing Spyware, Viruses And Other Malware From Computers
www.ictknowledgebase.org.uk/removingmalware/

End point security

The rise of relatively cheap consumer devices such as iPods, USB memory sticks, iPhones, Smart Phones and more, has increased the risk of intentional and unintentional data leaks and other malicious activity. It is easy for an employee to simply walk in and copy large amounts of sensitive data onto an iPod or USB stick or install PUPS (Potentially Unwanted Programs - legal or otherwise). For example, iTunes installs a copy of all the users music in the user profile and slows down the loading of it when the computer starts up. The administrator could lock down all ports but this is a difficult and pointless solution.

Once again the Acceptable Use Policy should state what activity is allowed – it may be acceptable for a staff member to copy over a file which they need to work on at home but is it OK for any member of staff to plug their phone or iPod into the network? For larger organisations, software can be run on the network which will protect from malicious activity emanating through USB connections.

Network misuse

Contrary to what a proportion of users might think, your computers and network are for the benefit of the organisation and not the individual. Using computers in a work situation for downloading or ripping music, viewing videos or listening to online radio is generally not a good idea – not only could it compromise the organisation if the downloads are illegal, it can also use up hard disc space and slows down internet connections to the organisation's detriment.

Obviously the boundaries of this

type of activity should be laid down in the Acceptable Use Policy as there are some genuine uses of web 2.0 tools which are of help to the voluntary sector. Some organisations will close ports on their firewalls to block services like Instant Messaging (Windows Live Messenger, Skype etc) because of misuse.

Use of filtering software or services (such as **OpenDNS** *www.opendns.com*) can also block sites or file types (see Web Threats). A service like OpenDNS routes all your web browser requests though their site and allows or disallows depending on how it has been configured by you. Configuration is easy and flexible (based on categories) and stops users "accidentally" stumbling upon sites of a dubious or illegal nature. In this way it can supplement and help enforce your acceptable use policy. Sites which are genuine but block because of the way the service works can easily be permanently or temporarily opened by the administrator.

Encryption

In simple terms, encryption is a way of "scrambling" information so that it cannot be read by anyone who does not have the necessary password or security key. Remember, that includes you if you lose or forget the password!

It is best NOT to send sensitive information by email as it could potentially be read by anyone en route to the intended recipient – it's a bit like sending a postcard.

However if you do feel the need to send sensitive data by email, be sure to use software to encrypt the message. Examples of free email encryption software include PGP (**Pretty Good Privacy**) available from the International PGP page at *www.pgpi.org*

For memory sticks and disks there are also free encryption tools available. These allow you to encrypt folders or whole drives including hard disks, memory sticks, and portable media such as DVDs. Examples include **TrueCrypt** available from *www.truecrypt.org*

Remember that any laptop can have any data on it stolen despite the presence of Windows passwords. Encrypting the disks in the laptop is the only way. BitLocker is great for this and is available in Vista and Windows 7 Enterprise & Ultimate Editions, which are not easy to get hold of but do implement **BitLocker** (and **BitLocker to go** for memory sticks) beautifully.

You also need a TPM (**Trusted Platform Module**) chip inside the laptop, this needn't mean paying a lot these days.

Bear in mind that as with any software, there's a bit of a learning curve involved in using encryption software so it can be a bit tricky to use, particularly for novices. So avoid sending sensitive data by email or storing it on portable media and devices.

Your organisation's Website

One area that is sometimes overlooked is the security of the organisation's own website. There are a number of issues which should be of concern:

- **General security**
  Make sure that you have details of the site's administrative passwords and, if necessary, FTP settings (for uploading revised pages, new information etc.) If your website was set up for you by a consultant web designer or volunteer, make sure they pass over details (and possibly change the password after they are done)

- **Backup**
  If your site is comprised of html pages ensure you have copies of them all on your own

computer or server (and back that up too!). If something happens to the site (host goes bust or gets hacked) then you'll need to be able to rebuild your site as quickly as possible. If it's a site using a Content Management System (CMS) then it will normally have some method of allowing you to download a zip file of the database which sits behind the site. Then back that up.

- **Hacking**
  The site could be compromised by an external intrusion causing total loss, or possibly infected with a virus. Ensure that the site is password protected (change from the default) and make sure you have that backup!

End of life

Whenever you are getting rid of computers including PCs and servers, you should ensure that the company collecting will guarantee to securely wipe all data from hard disks before refurbishing or recycling. Use only licensed or accredited companies. As a precaution you should delete all files and reformat hard disks before disposal (although be aware that this is not enough to make your data irrecoverable, a better approach might be to use cleaning software such as **Eraser** *http://eraser.heidi.ie/*

Some organisations will have a policy of offering old working equipment to staff members or friends. Whilst this is a great way of avoiding waste you should still ensure that all data is wiped from the disk.

If your data is highly confidential or sensitive you should consider removing hard drives (and possibly even destroying them) before letting them off the premises (although this, and removing RAM, makes them less useful to the recyclers).

As a policy, ensure that all user data is stored on the server if you have one as it makes it less likely that sensitive information will find its way out into the wild. If you are replacing servers, once the data has been migrated over, we suggest that you hang onto the hard drives which are usually easy to remove and keep in a safe (or safe place).

Knowledgebase

Disposing Of Old Computer Equipment
www.ictknowledgebase.org.uk/disposingoftechnology/

Part 4 - Resources and further information

Books

Network Security for Dummies - Chey Cobb, published by John Wiley & Sons

Vista Security for Dummies - Brian Koerner, Mike Borkin, and Joe Howard, published by John Wiley & Sons

Firewalls for Dummies – Brian Komar, published by John Wiley & Sons

Network Security Assessment: Know Your Network – Chris McNab - published by O'Reilly

IT Governance: A Manager's Guide to Date Security and ISO 27001 / ISO 27002 – Alan Calder – published by Kogan Page

From Nightmare to Nirvana - an ICT survival guide for trustees – available on paper or downloadable from *www.icthub.org.uk/publications/#management*

A Guide to Managing ICT in the Voluntary and Community Sector - available on paper or downloadable from *www.icthub.org.uk/publications/#management* or online at *www.icthub.org.uk/managing_ICT/*

Events

InfoSecurity Europe is the ICT security industry's annual exhibition and conference which is held in London in the spring at Olympia or Earls Court. See *www.infosec.co.uk*

Magazines/Journals

InfoSecurity magazine – published 7 times/year by Elsevier. Sample copies from *www.elsevier.com*

Websites

In addition to those mentioned in the text, the following may be useful:

ICT Knowledgebase – *www.ictknowledgebase.org.uk*
Over 300 articles on all aspects of ICT management and use

ICT Suppliers Directory – *www.suppliersdirectory.org.uk*
Over 100 independently verified companies providing ICT services to the sector

TechSoup – *www.techsoup.org*
Technology resource aimed at nonprofit organisations

Jericho Forum – *www.opengroup.org/jericho/*
ICT security think tank

Business Link – *www.businesslink.gov.uk*
Factsheets for small businesses on ICT security, which are equally relevant to the VCS

Idealware – *www.idealware.org*
Comparison reviews of software and services

1. Physical and environmental risks

Risk description	Reducing Risk
Theft of equipment from staff areas and Theft of equipment from public areas	Insurance (applies to all topics) Physically locking down with cables etc Record serial numbers Burglar alarm/bars, window locks General office security, know who's on site etc Marking equipment (Selectamark) Policy and rota for locking up Lockable cabinets Monitoring Cameras Choose the asset tag with customer details when ordering new computers.
Theft of equipment off the premises (e.g. laptops)	Check insurance coverage for offsite Staff awareness Usage policy Password protection Lock in secure cabinet when in office Do you really need to use the laptop or can you just take data with you on memory pen, CDR? Sign in and out procedure Laptop lock cable at home Use non attractive laptop carry case
Fire!	Good backup policy Policy for equipment use Fire alarms/extinguishers (ensure staff know which type of extinguishers to use on electrical equipment) Sprinklers (ensure critical equipment cannot be affected by water damage) Portable appliance testing (reduce risk of electrical fires) Don't leave equipment on standby Fireproof safe important documentation Fire proof server cabinet Smoke detectors
Flood	Keep equipment away from water sources (pipes etc) Raise equipment off ground "Flood rescue policy" – or disaster policy

2. Data risks

Risk description	Reducing Risk
Files being deleted accidentally	Regular backup and restoration check (applies to most topics) Backup policy (ditto) Staff training and awareness (ditto) Passwords/restrictions Read only folders Enable shadow copies on windows servers Training and induction for staff
Files being deleted maliciously [e.g. by discontented staff (or ex-staff)]	Folder permissions Account management (change passwords) Contracts and policy
Files being corrupted or infected by viruses	Anti virus (install, run, update automatically & check) Firewall updates Disk maintenance Staff awareness of virus activity and suspicious emails
Files being viewed by unauthorised staff	Permissions Log on screen savers, lock workstation when away from desk
Users installing unlicensed (or unapproved) software	Acceptable use policy Group policies Block download access through firewall Management of licences/software media resources etc Operating system tweaks
Database alterations by unauthorised staff	Passwords on database access Access restrictions Configurable permissions for users e.g. read only etc. Policy and training
Data being viewed by contractors	Confidentiality policy/agreements Contract
Loss of data on mobile devices e.g. memory keys, CDRs, Portable Hard drives, floppy disks	Don't put anything important or irreplaceable on mobile devices Security programs Encrypted USB memory keys Thumb print recognition Don't use as whole-system back up devices

3. Breakdown and maintenance risks

Risk description	Reducing Risk
Hard drive crashing or dying – risk of data loss	PC and server warranties (applies to all topics) Plan ahead financially and strategically (ditto) Tech support and Service Level Agreement (SLA) (ditto) Regular maintenance (policy issue) Spare disc/redundancy/RAID (Redundant Array of Independent Disks) on server Back up Don't keep important stuff on PC drives if have server
Power supply dying	Surge protectors on PCs UPS (Uninterruptible Power Supply) on server and critical PCs Redundant power supply on server. Run self test on UPS every quarter
Memory failing	Check event logs for errors Replace hardware as policy
Other failures- motherboards, drives, graphics cards etc.	As above Data recovery costs (high!)
Operating system (OS) unsupported (e.g. Windows 95, 98, NT Workstation, NT Server)	Upgrade to supported OS If can't then ensure firewall etc. is secure
Potential security risks through operating system not being updated	Download and install automatic updates Service packs Check updates are being applied

4. Network security risks

Risk description	Reducing Risk
No log on passwords	Policy issue Set up and change regularly! Use unusual/varied passwords not names, postcodes etc Complex server password Set up on server for agreed period (e.g. 3 months)
Server being used for spam relaying	Firewall Maintain firewall Mail server settings to disable spam relay functionality
Unsecured wireless network	Set WEP (Wireless Encryption Protocol) security (as minimum) Consider cabling? Secure SSID (Service Set Identifier) broadcasts (change name of SSID from default)
Staff able to plug in unsecured USB (Universal Serial Bus) devices	Policy Block USB ports/CDROM/Floppy Scan any media plugged in using security monitoring program (large orgs only)
No passwords (or defaults being used) on routers and firewalls	Password protect / change password from default

5. Internet use risks

Risk description	Reducing Risk
Email used for sending confidential information	Email/Internet Policy (applies to many topics below) Encryption/digital signature/ certification Use alternatives such as fax or post Password-protect documents
"Pop-ups" and browser hijacks (malicious software installs and takes over your web browser)	Use alternative browser such as Firefox Pop up blocker Anti-spyware programs – install, run regularly and update
Spam	Anti-spam software Don't publish easily harvestable addresses on website Don't send mail to multiple Use third party mail hub to filter emails like (message labs)
Phishing attacks (directing you to fake websites that try to steal information such as credit card numbers)	Policy/awareness by staff Anti-spam software
Online purchasing of personal items	Blocking of secure sites (firewall) Blocking through use of software or online service Request invoices for good rather than using credit cards
Visiting unsecured or offensive sites	Policy Blocking through use of software or online service
MSN Messenger for personal or unauthorised use	Can be blocked on firewall but can also be got around due to behaviour of MSN

For an explanation of any unfamiliar terms try the Knowledgebase Glossary
www.ictknowledgebase.org.uk/index.php?id=46

ICT Risk Assessment Checklist

The checklist contains a number of elements each of which addresses a different aspect of computer security or risk and is important for protecting your organisational data and computing resources. The elements are presented below in the initial checklist, each with a question to prompt consideration.

After reviewing the element, record your initial assessment by checking the appropriate box on the checklist:

OK - the element has been addressed by the organisation action or policy. All the detailed questions can be answered affirmatively.

Review - The basic issue has been addressed, but further review is warranted. Not all the detailed questions can be answered in the affirmative.

Requires Immediate Attention - The element has not been addressed or recently reviewed. Few, if any, of the detailed questions can be answered in the affirmative.

Upon completion, the checklist provides a profile of your organisation's data and computing resources security. Those elements assessed as "Requires Immediate Attention" constitutes the organisation's primary security vulnerabilities and should receive prompt attention. A majority of "Review" or "Requires Immediate Attention" assessments suggests the organisation would benefit from a more systematic risk assessment and analysis.

Element	OK	Review	Now!
Physical Security • Is our computing equipment properly secured? • Is there public access to our systems – and is it secure?			
Account & Password Management • Do we ensure only authorized personnel have access to our computers? • Do we require and enforce appropriate passwords? • Do we have appropriate permissions on folders and/or files?			
Virus Protection etc. • Do we use, and regularly update, anti-virus software? • Do we use and regularly update anti-spyware software? • Do we have anti-spam measures in place?			

Element	OK	Review	Now!
Physical Security • Is our computing equipment properly secured? • Is there public access to our systems – and is it secure?			
Account & Password Management • Do we ensure only authorized personnel have access to our computers? • Do we require and enforce appropriate passwords? • Do we have appropriate permissions on folders and/or files?			
Virus Protection etc. • Do we use, and regularly update, anti-virus software? • Do we use and regularly update anti-spyware software? • Do we have anti-spam measures in place?			
Data Backup and Restoration • Do we periodically backup individual and organisation's data? • Do we test restoring data from backup media? • Do we keep backups offsite? • Do we keep onsite back ups in a secure, fireproof area?			
Operating Systems • Are the operating systems we use on our workstations and servers updated with security "patches" and service packs?			
Application Software • Are our common applications (e.g. databases, accounts package) configured for security?			
Confidentiality of Sensitive Data • Are we exercising our responsibility to protect sensitive data under our control?			
Disaster Recovery and backup • Do we have a current disaster recovery plan? • If we have one, has it been tested? • Do you have backup procedure in place? • If yes, has it been tested?			

Element	OK	Review	Now!
Security Awareness and Education • Do we have safe computing policies and procedures in place? • Is our management committee/board aware of the issues? • Are we providing information about computer security to our staff?			
Network and server security • Do we have a firewall on our broadband connection? • Does our server have redundancy e.g. mirrored hard drives, RAID, redundant power supplies? • Is our network fully documented? • How good are we at managing our user accounts e.g. deleting ex-staff members accounts, changing passwords regularly? • Is our wireless network secure? • Is our remote access/VPN secure?			

Computanews now accepts advertisements

If you offer a technology product, service or event aimed specifically at the voluntary sector you can draw attention to it through the pages of **Computanews**.

Computanews is a specialised magazine covering the use of technology within the voluntary sector. It has a key audience of:

- organisation managers and trustees
- staff responsible for their own organisation's IT
- Circuit Riders who provide advice and technology support to other organisations

Computanews rates:

- 1/8 page £60
- 1/4 page £100
- 1/2 page £180
- 1 full page £300

A 10% discount applies if advertising in multiple issues.

The circulation of **Computanews** is currently around 2,500 copies per issue, distributed 4–6 times a year. We anticipate that the circulation will increase now that it is becoming available as a free, downloadable file.

To place an advert, or for more details about rates and dates, please email: **computanews@lasa.org.uk**
or phone: 020 7426 4473

Looking for ICT support in Cumbria?

IT4Cumbria is an innovative, all-round ICT support service provided through Cumbria CVS

- Telephone support
- Network, PC and server maintenance
- System planning
- Web design and hosting solutions
- Remote access solutions
- Equipment hire

For more information call: 0845 5212268
Email: info@it4cumbria.org.uk

appiChar
FOR ALL YOUR IT NEEDS

Managed IT services for the not-for-profit sector

Greater control over your budget with appiCard

appiCard is a **NEW** fixed rate IT service that provides assigned not-for-profit employees and volunteers with direct, immediate and unlimited access to expert IT Support.

Services included in the appiCard:

appiCard	Included?
Unlimited telephone support	✓
On-site critical support	✓
Online backup per person	✓
Remote monitoring	✓
Workstation and asset management	✓
Total printer cover telephone and critical onsite	✓
Liaison with 3rd party branded application software suppliers	✓

To discuss further: 0845 456 3970 | info@appichar.co.uk

www.appichar.co.uk

ICT Security Guide

Lasa services

knowledgebase
independent ICT information + advice
www.ictknowledgebase.org.uk

SUPPLIERS DIRECTORY
connecting you with trusted technology suppliers
www.suppliersdirectory.org.uk

uk circuitriders
voluntary sector technology support
http://ukriders.lasa.org.uk

aims
advice + information management system
www.lasa.org.uk/aims

multikulti
information + advice in community languages
www.multikulti.org.uk

rightsnet
the welfare rights website for advisors
www.rightsnet.org.uk

Supported by

BIG LOTTERY FUND

LOTTERY FUNDED

About Lasa

Established in 1984, Lasa has provided ICT advice to the voluntary sector for 25 years. Its two main aims are to promote social inclusion through access to social welfare law, information, advice and guidance; and to promote an efficient and effective sector through improving access to impartial ICT advice and support resources – such as Computanews and the London e-bulletin (www.lasa.org.uk/lasa/mailing-lists)

Our online ICT Knowledgebase (www.ictknowledgebase.org.uk) is a comprehensive source of independent expert ICT advice for VCS organisations, now containing over 300 articles. The Suppliers Directory (www.suppliersdirectory.org.uk) connects VCS organisations with over 150 approved suppliers of ICT products and support services across England. Lasa is also noted for its consultancy work and leadership in developing the Circuit Rider model of local ICT support. (http://ukriders.lasa.org.uk/)

Our funders

Big Lottery Fund
Capacity Builders
The City Bridge Trust
City Parochial Foundation
Cripplegate Foundation
Esmée Fairbairn Foundation
The Law Society Charity
Legal Services Commission
London Councils
The London Legal Support Trust
Wates Foundation

Credits

This Guide has been mainly sourced from articles available on Lasa's ICT Knowledgebase and we thank the authors of the original articles.

The Guide was edited by Aba Maison and Ian Runeckles of Lasa with additional input following peer review from Morgan Killick of ESP Projects (www.espprojects.co.uk) and Maher Al-Ugaily of Superhighways (www.superhighways.org.uk) to whom thanks. Design by Miles Maier at Lasa. Cartoons by Phil Evans.

Lasa
Universal House
88-94 Wentworth Street
London E1 7SA

www.lasa.org.uk/ict
computanews@lasa.org.uk
020 7426 4496

Registered charity no: 800140

Published: October 2009

lasa