Information Security

Policy and Guidance For schools

Helping you safeguard Council, school and pupil information and ICT equipment

November 2013

Contents

The policy section of this document was amended for schools from the Kirklees Council Security Policy (February 2008)

Rationale

Several high profile instances of data loss have been reported in the press recently and as a result organisations are tightening up their procedures for handing personal and confidential data to prevent any further occurrences. This applies equally to schools and school staff with access to such data – indeed, it is currently common practice for school staff to have personal and confidential information about pupils, staff or parents on their personal laptops, home computers, USB memory sticks and other media. Generally, that data is not held securely and these guidelines are provided to help schools tighten up their own procedures.

In September 2008 Becta produced guidance; **Good Practice in information handling in schools; Keeping data secure, safe and legal** [6.29] The underlying principle of the guidance is that schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. The following is a summary of the main points from that document :

- The head teacher will take responsibility for the security of information in the school.

- South Crosland C.E. Junior School identify their information assets to ensure they know:
  - What information they hold and for what purpose
  - How it is amended or changed over time
  - Who has access to it and why

- South Crosland C.E. Junior School needs to make short term changes and plan for longer term changes to systems and operations to ensure that data is protected following the schools own risk assessment. e.g
  - Providing data handling awareness training
  - Providing encryption
  - Planning for incident response
  - Provision of secure remote access
  - Review of contract clauses for data protection
  - Formal reviews of all user access requirements to sensitive data

- Good practice recommendations include:
  - All sensitive data must be correctly labeled
  - Sensitive or personal data should not be removed from the school premises unless the media is encrypted and is transported securely for storage in a secure location.
  - When data is required by an authorised user from outside of the school premises – for example by a teacher working from their home – they should have secure remote access to the management information system (MIS) or learning platform.
  - All desktop, portable and mobile devices, including media, used to store and transmit personal information should be protected using approved encryption software.
  - All data in transit must be protected, however it is being moved
  - Sensitive or personal data should be securely deleted (over-write media, destroy CD/DVDs, or shred paper) when it is no longer required. All data should be kept safe and made available only to those who are authorised to access it.

- There must be a process in place for dealing with potential security incidents

Relatively easy steps can be taken to address the majority of these recommendations and these will be considered further in this document, first within a policy context and secondly as practical guidance .

This document will be reviewed regularly to take account of changes in this rapidly developing area.

Introduction

This Information Security Policy document summarises what is expected of all school staff in the course of their duties and while on school premises in relation to information security and computer equipment.

Its aim is to protect:

- staff, pupils, parents and visitors;
- assets, including information assets;
- the school's finances and reputation

by reducing the risk of:

- harm to individuals
- accidental loss or damage to assets
- unintended change to, or disclosure of, personal and confidential information
- deliberate and harmful acts carried out through lack of awareness of their consequences.

It applies to:

- all services in the school
- all employees of the school, both permanent and temporary
- pupils
- any other person working for the school or on school premises.

This policy document provides the information necessary to enable staff and others to meet their general responsibility to safeguard the school's information and other assets.

The guidance section of this document in the Appendix describes a number of practical ways in which schools and individuals can protect their data and prevent accidental loss, disclosure and misuse.
Any reference to personal data in this document means private, personal or confidential information, whether in electronic or written form, about identifiable pupils, families, employees, members of the public or any other persons.
A large amount of background and support material is available from the Kirklees Council Information Management policy [6.11] which is widely referenced in this document, including a useful summary leaflet called "Information Security" which could be used for staff induction. [6.1]

1 Organisational Security

1.1. School leaders, including governors, are responsible for the physical security of the school site and there must be a school policy to comply with the relevant health and safety regulations. (See school Health and safety policy) [6.23, 6.24]

1.2. In addition to this, we have a duty to safeguard staff and pupil's personal data stored and transmitted electronically. Our senior management team is responsible for developing and implementing policy and advice covering information security issues and ensuring that the policy is consistent with other related school policies and guidance such as those covering Health and safety, Recruitment and Selection and ICT [6.4, 6.5, 6.6, 6.7, 6.8].

1.3. We should also be aware that arrangements for safeguarding pupil data are part of the overall requirement for safeguarding procedures which are reported in the SEF. These include ensuring safe use of the internet by staff and pupils and acceptable use policies which should be covered in the school e-safety policy for pupils and staff [6.22].

1.4. Tasks for SMT will include :

- identifying and managing risks and issues of concern
- coordinating a response
- disseminating and reviewing advice.

1.5. All staff must ensure that those who report to them are aware of their general responsibilities in respect of security and the value of information, and of any issues or risks specific to their areas of responsibility.

1.6. Information security should remain a regular item on staff meeting agendas/briefings and includes the administrative and support staff to ensure that issues of concern are highlighted and addressed.

1.7. We have developed a disaster recovery plan for their ICT systems to cover the possible loss of data as a result of theft, fire, flood, electrical failure and accidental or malicious acts.

1.8. We ensure that secure arrangements are made for any copies of personal or confidential data taken off the school site.

1.9. Advice on issues related to data security can be found on Kirklees Ednet [6.22] or by contacting ITCAS.

2 Personal Security

2.1. General responsibility for information security must be included in the induction procedures for all staff. [6.5, 6.7]

2.2. Contractual arrangements with staff and supply agencies require appropriate checks on agency staff. [6.5, 6.6, 6.8]

2.3. External contractors, consultants, trainers, temporary teachers and others employed on school premises or given access to school systems are subject to checks and agreements appropriate to the services to be provided. [6.2, 6.3, 6.12, 6.13, 6.14, 6.15]

2.4. Work placements, students, volunteers, parents, carers and any other persons not subject to a contract of employment, and having access to school computer systems, including remote access, are subject to confidentiality and security agreements.

2.5. Supply or temporary staff working in the school for short periods of time are not be provided with log-ins to systems which allow them access to sensitive data, for example G2, SIMS or the school learning platform. Furthermore, paper records should be treated with the same caution sharing only the minimum amount of data for them to do their jobs effectively. [6.5, 6.6]

2.6. A record is made of equipment, fobs etc, issued to new employees and anyone else listed in paragraphs 2.4 and 2.5.

2.7. Induction training for all staff must includes security and data protection. Similarly, curriculum activities are provided for pupils to acquire the knowledge and understanding about safe use and management of their personal information. [6.5, 6.7]

2.8. On termination of employment, all school property must be returned or accounted for. Email, school network, and other system access must be cancelled. Passwords protecting sensitive data must be changed. [6.7]

3 Security of Information

3.1 Information is an important school asset and it must not be assumed that it is a common resource to be freely exchanged.

3.2 Under Freedom of Information legislation, most information is available to the public on request, subject to specific limitations and exemptions, in particular :

- information held in confidence
- personal data which can only be disclosed to the person or their legal guardian, unless there is consent or a legal requirement.

(cf. school policies for Data Protection and Freedom of Information legislation.)

Further guidance on the Freedom of Information Act and data protection is available. [6.25, 6.26]

3.3 All information, whether disclosable or not, is protected from accidental and malicious loss or damage. Personal and confidential information is protected from unintended access and disclosure.

3.4 Every personal dataset routinely shared with an external agency is the subject of a sharing agreement based on agreed protocols adapted to the particular circumstances and the nature of the information being shared. Each agreement defines the method of transmission (e.g. Groupcall, Anycomms, S2S) and the security measures are employed to ensure the safe delivery of the information. Agreed security measures are rigorously monitored and enforced by the responsible managers. [eg 6.12, 6.13, 6.14, 6.15]

3.5 The school holds a central register of all data-sharing agreements and ensure that relevant staff are aware of the existence of any such agreements, and of their terms and scope.

3.6 Outside the terms of a data-sharing agreement, personal data may be disclosed only to persons who can show they have a right to it.

3.7 Personal data should not be accessed or viewed without legitimate reason. Under no circumstances will personal data held by the school be accessed, viewed or used for any private purpose.

3.8 Personal data should only be stored on secured network drives, secure PCs and laptops or in a secure on-line system such as Integris G2 or Digital Brain, which require user authentication (log in name and password) to access the data.

3.9 All personal data stored electronically is systematically backed up as part of normal network management or by copying from stand alone machines to external media e.g. CD/ DVD. Secure storage of these backups is essential.

3.10 Personal data held on laptop computers and portable storage devices (e.g. USB memory sticks) is protected to prevent unauthorized access. It is not be kept for longer than is necessary for its intended purpose and it is deleted after use or transferred to the network or CD/DVD and stored securely.

3.11 Protection can be provided in a number of ways. For example :

- Laptops must have log in and password authentication
- Encryption should used where possible – on individual files, portable storage devices, or whole computers
- See Appendix : Practical guidance for protecting information.

3.12 We keep a secure record of all passwords used to encrypt sensitive data so that data can be recovered if a member of staff leaves.

3.13 We have a secure system for resetting passwords.

3.14 Personal data transferred to a portable device is removed before the device is made available to another person.

3.15 Care is taken to ensure that all personal and confidential information in paper files is securely stored at all times when not in use. Such documents should be correctly labeled as confidential following BECTA guidelines.

3.16 We ensure that sensitive documents sent through the post are sent by the most secure means available e.g. registered post.

3.17 Email and fax are insecure media for transmitting personal and confidential information and is avoided where an alternative exists. The sender is always responsible for ensuring that email addresses and fax numbers are correct, and that the intended recipient of a confidential fax is notified before it is sent. Staff are aware that forwarding emails to personal email addresses could further reduce their security.

3.18 In the exceptional circumstances where personal data has to be shared by email, the data must be sent as securely as possible for example by encrypting the attached data file using a strong password shared verbally (see later advice).

3.19 Documents containing personal or confidential information are disposed of by shredding. Paper containing personal data is not re-cycled or used as scrap.

3.20 Documents, media, redundant PCs and similar equipment for disposal should be stored securely until removed for disposal. All ICT equipment should be disposed of in accordance with appropriate legislation. See Becta guidance on how to dispose of redundant equipment [6.28].

3.21 PCs, laptops and other devices are not disposed of until all personal data has been securely removed using specialist software. Data stored on PCs cannot normally be permanently deleted using the 'Delete' command or by reformatting. Software such as ‘Eraser’ (http://www.heidi.ie/node/6) could be used but if in doubt advice on the permanent removal of data should be sought from InTech or other specialist companies when disposing of PCs containing personal data.

3.22 CDs/DVDs and floppy discs no longer required should be destroyed. Data on disposable electronic media cannot normally be permanently deleted, and any unwanted media containing personal data must be physically destroyed, with due regard for personal safety. CD/DVD shredders are now available to help destroy discs safely. (An idea of the range available can be seen at : http://www.shreddingmachines.co.uk/cd_shredders.asp?id=1&sec=CD/DVD%20shredders)

3.23 When working with personal and confidential data computer screens are positioned where they are not visible from outside the immediate work area.

3.24 Anyone transferring personal data from school sources to their own personal computer or memory stick is personally liable for the security of that data and for any legal consequences.

3.25 We ensure that the network is as secure as possible to prevent unauthorised access.

3.26 Work at home must be carried out with similar consideration for security as office-based work. All staff working off the school site or at home are aware of the additional and significant risks of :

- information 'leakage' through being overlooked or overheard
- the opportunity for hacking presented by Bluetooth or wi-fi
- leaving sensitive school data accessible on home computer systems.

3.27 Staff using their own home computers for school work must transfer and delete the data at the end of the working session : home computers should not be used to store personal data from school. The minimum amount of data should be taken home. Staff must also ensure that their home wireless network is security protected. Bluetooth should never be used as a means to transfer sensitive data.

3.28 Great care is taken when collecting personal data from pupils for curriculum use to avoid potential problems arising from the data.(e.g. developing a database on pupils' personal characteristics.) Such data is covered by the data protection act and parental permission may be needed to collect it. At the very least the data should be "anonymised" so that no-one can be identified personally. Never collect any characteristics which are attributable to simple genetic traits (such as eye colour). Individuals have the right to know what is stored about them, what it is used for, how secure it is, how long it is stored and when it is removed. This has implications for the primary curriculum, in particular common database activities .

3.29 Any staff member becoming aware of an incident that could compromise data security should report it to the head teacher. Such incidents include, but are not limited to :

- unauthorised access or attempted access to computer systems
- unauthorised access to personal data in any medium
- accidental loss or disclosure of personal data

These issues should be covered in the school's e-safety guidance.

4 Physical Security

4.1. The security of school premises, pupils and staff will be covered in other school policies, including expectations regarding locking doors, windows, cupboards, challenging visitors, etc.

4.2. Consideration should be given to the use of ICT equipment to control access to different parts of the building e.g. fobs.

4.3. Consideration should be given to the physical security of pupils and staff when carrying portable ICT equipment to and from school and around the school site. For example, pupils should not carry bags which are easily identifiable as laptop cases.

5 Computer Security

5.1. Every adult user of the school network and stand alone computers has their own user name and password.

5.2. Access to all computer applications involving personal data must be controlled and protected by secure passwords. Passwords should never be shared (except in circumstances covered in 5.5). Passwords should never be automatically saved by the computer or internet browser.

5.3. No external party, supplier, technician, bureau or other agency are given access, either in school or remotely, to systems, data, hardware or networks unless an appropriate access agreement is in place to ensure they understand their responsibilities.

5.4. Staff user passwords, such as those for logging on to the network or school systems, provide an accountability trail and they :

- must not be recorded or shared with any other person or saved by the computer
- must not be written down in a manner discoverable by any other person
- must not contain numbers substituting for letters (eg al3x, fel1x)

System passwords, such as for the Administrator's Account, and passwords which are used for sharing a secret (e.g. file encryption passwords to protect sensitive data) are recorded and stored securely by the headteacher.

5.5. Staff should take care to ensure that ICT equipment is protected against theft. All equipment is security marked, physically secured where possible, or stored in locked cupboards and never left unattended. Equal care should be given to protect equipment taken off site or home. For example, laptops should never be left on view in a car. The equipment is insured against theft or loss and it must be clear who is responsible for providing insurance

5.6. We have robust procedures in place to ensure that all PCs and laptops, including those not connected to the school network, are regularly backed up and have up to date firewall, anti-virus, anti-spyware and security updates installed.

5.7. To avoid the risk of virus infection, emails that are obvious spam or with unsolicited or unexpected attachments should not be opened.

5.8. Software should only be installed on a school computer in accordance with the school's policy (which will cover issues such as licensing, open source, use at home, inventory, etc).

5.9. Hardware (such as Bluetooth and wi-fi adapters and personal laptops) should only be installed or attached to the school's network in accordance with the school policy due to the risk from hacking and virus infection.

5.10. If a virus is suspected then technical advice should be sought immediately.

6 Related Policies and Documents

	Policy/document	Source
6.1.	**Information Security leaflet**	http://intranet/business/documents/pdffiles/infosecurity/InformationSecurityleaflet.pdf
6.2.	**Working with external parties (including guidance on how to produce a data-sharing agreement)**	http://intranet/business/documents/pdffiles/infosecurity/chapter4/externalparties.pdf
6.3.	**Data Sharing protocols**	http://intranet/managers/process/ikm/GenericProtocolInfoExchange.pdf
6.4.	**Employing young people**	http://intranet/business/documents/PDFFiles/youngpeople.pdf
6.5.	**Personnel security (recruitment, induction, responsibilities, incident reporting, etc)**	http://intranet/business/documents/PDFFiles/infosecurity/chapter6/personnelsecurity.pdf
6.6.	**Safer recruitment and safeguarding**	http://www.kirklees-ednet.org.uk/management/HR/safeguarding.htm
6.7.	**Employee induction, termination and transfer checklist**	http://intranet/business/documents/PDFFiles/forms/terminationchecklist.pdf
6.8.	**Contract Letter clauses on Information Security**	http://intranet/business/documents/PDFFiles/infosecurity/ContractLetterClausesOnInformationSecurity.pdf
6.9.	**Incident reporting template**	http://intranet/business/documents/pdffiles/infosecurity/incidentreportingtemplate.pdf
6.10.	**Use of Electronic Communications for school staff Policy**	http://www.kirklees-ednet.org.uk/subjects/ictgeneral/management/policies/ELECTRONIC-COMMUNICATIONS-FOR-ALL-SCHOOL-STAFF1.pdf
6.11.	**Information security guidelines**	http://intranet/managers/process/ikm/infosecurity/infosecuritymenu.shtml
6.12.	**Bureau services security agreement**	http://intranet/business/documents/pdffiles/forms/BureauServicesSecurityAgreement.pdf
6.13.	**On site systems security agreement**	http://intranet/business/documents/pdffiles/forms/OnSiteSystemsSecurityAgreement.pdf
6.14.	**Remote access systems security agreement**	http://intranet/business/documents/pdffiles/forms/RemoteAccessSystemsSecurityAgreementSecureShell.pdf
6.15.	**Remote Access Systems Security Agreement (VPN)**	http://intranet/business/documents/pdffiles/forms/RemoteAccessSystemsSecurityAgreement.pdf
6.16.	**Identity cards**	http://intranet/staffinfo/IDcards/idcards.shtml
6.17.	**Equipment disposal**	http://intranet/internalservices/enviromanagement/recycling/recycle.asp
6.18.	**Anti-fraud**	http://intranet/business/documents/HTMFiles/antifraud.shtml http://intranet/business/documents/HTMFiles/fraud.shtml
6.19.	**Bomb threats**	http://intranet/business/documents/HTMFiles/bombthreats.shtml
6.20.	**CCTV**	http://intranet/managers/process/ikm/dataprotection/Documents/CCTVStandardsandProcedures.pdf
6.21.	**Disaster Recovery plan for ICT**	http://www.kirklees-ednet.org.uk/subjects/mis/general.asp
6.22.	**e-safety guidance**	http://www.kirklees-ednet.org.uk/subjects/ictgeneral/esafety.htm
6.23.	**Governor Information sheet on Health and safety**	http://www.kirklees-ednet.org.uk/management/governors/documents/infosheets/index.htm
6.24.	**Health and safety guidelines for schools**	http://www.kirklees-ednet.org.uk/subjects/health/documents.htm
6.25.	**Data protection policy**	http://intranet/business/documents/HTMFiles/protection.shtml
6.26.	**Freedom of Information**	http://www.kirklees-ednet.org.uk/management/fia/guidance.htm
6.27.	**Personal Use of Equipment**	http://www.kirklees-ednet.org.uk/management/personel/38.pdf
6.28.	**Safe disposal of redundant equipment**	http://schools.becta.org.uk/index.php?section=re&catcode=ss_res_eva_02&rid=3811
6.29.	**Good practice in information handling in schools. Keeping data secure, safe and legal**	http://schools.becta.org.uk/index.php?catcode=ss_lv_saf_dp_03&rid=14734&section=lv

7 Legal Context

Data Protection Act 1998 http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1	Defines personal data and regulates all aspects of its use and processing.
Computer Misuse Act 1990 http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm	Prohibits unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences, and unauthorised modification of computer material.
Copyright, Designs and Patents Act 1988 http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm	Covers the copying of proprietary software
Regulation of Investigatory Powers Act 2000 http://www.opsi.gov.uk/acts/acts2000/20000023.htm	Part III: Investigation of electronic data protected by encryption etc.
Freedom of information Act http://www.dca.gov.uk/rights/dca/foidcaintro.htm	Covers the right of access to information
Disposal of Equipment WEEE http://www.netregs.gov.uk/netregs/275207/1631119/	Covers safe disposal of redundant electrical equipment

Appendix

Practical guidance for schools to protect information

To help protect data on your computer, you should secure individual files and folders and take steps to secure the physical computer itself. If the computer contains sensitive information, you should keep it in a safe location. Other ways to secure your computer include locking it whenever you are away from your desk, setting up a password-protected screen saver and encrypting your equipment and files. The school should ensure there are no generic users on the system so there are no unprotected "back doors" and only senior staff, IT staff and network administrators should have administrative rights (these are high level users able to reset passwords, remove user accounts, etc.).

This Appendix aims to provide a range of precautionary measures which can be taken to protect computer systems. Some of this advice is, of necessity, quite technical in nature and several sections, which are specifically identified, should only be attempted by IT technicians or those with a good technical understanding. The following table indicates those tasks which can be undertaken by anyone with basic ICT skills and those which require more technical competence.

	Admin/ Office	Admin/ Class	Staff Laptop	Home computer	Technical
1. Use strong passwords	✓	✓	✓	✓	✓
2. Lock your computer	✓	✓	✓	✓	✓
3. Screensaver with password	✓	✓	✓	✓	✓
4. Set up your computer securely	These tasks will be done by the school ICT technician.				
a) Install AntiVirus software			✓	✓	✓
b) Install Antispyware software			✓	✓	✓
c) Set up a Firewall			✓	✓	✓
d) Install Windows Critical Updates			✓	✓	✓
e) Use secure User Accounts			✓	✓	✓
f) Switch off Guest Account			✓	✓	✓
g) Set strong password and account policy					✓
h) Make files private			✓	✓	✓
i) Do not use the Shared Folder			✓	✓	✓
j) Set up secure Internet Explorer settings					✓
k) Use NTFS file system					✓
l) Disable Bluetooth					✓
5. Set up your home wireless network securely					
a) Configure the wireless router					✓
b) Connect computer to network			✓	✓	✓
6. File Encryption	These tasks will be done by the school ICT technician.				
a) AES encryption			✓	✓	✓
b) Zip encryption					
i) 3rd Party applications			✓	✓	✓
ii) Windows Zipped Compressed Folders					✓
7. Device Encryption					
a) Encrypted volumes (eg. Truecrypt)			✓	✓	✓
b) Whole device encryption					✓
c) Hardware encrypted USB flash memory					✓
d) Windows XP Pro Encrypted File System					✓

1. Use strong passwords

Wherever you use a password (such as logging on, setting a screen saver, encrypting or zipping files, securing the computer Administrator user account, etc) your security is only as good as your password and the measures you take to ensure that your password is not disclosed to unauthorised third parties. To be as secure as possible you should give careful thought to your password and make it as strong as possible by following the simple rules described below. You should never allow the computer to automatically save your password.

All passwords should :

a) be at least 7 characters long - the most secure passwords are at least 14 characters long. Windows XP passwords can be up to 127 characters long. Increasingly, people are using pass*phrases* rather than pass*words*.
b) contain a combination of characters from the following groups :
   - letters A-Z, a-z (note : uppercase and lower case letters are different characters in most systems)
   - numerals 0-9
   - symbols ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
c) have at least one symbol character somewhere in the middle
d) be significantly different from prior passwords
e) not contain your name, family names or user name
f) not contain the birthday of you or your family
g) not be a common word or name
h) not contain anything else which is easily guessed (such as addresses and telephone numbers)
i) not contain numbers substituting for letters (eg 1 for I, 3 for E, etc)

Password-guessing software uses one of three approaches: intelligent guessing, dictionary attacks, and brute force that tries every possible combination of characters. Given enough time, the brute force method can guess any password. However, it can still take years to guess a strong password. The best encryption systems are based on key generation and passwords can be whole sentences. These passwords can take millions of years for supercomputers to decipher.

Caution

Before storing any copies of critical information in encrypted form, you should carefully consider the risks associated with losing or forgetting the passwords because the data will be unrecoverable. Schools must keep a record of the passwords you use and keep this record in **a secure place** (eg in the school safe).

If a keystroke monitor or other malicious code (such as a virus) is running on your computer, your password may be recorded when you type it. Be sure to check frequently for viruses and follow other recommended computer safety procedures (such as firewall settings and spyware removal).

2. Lock your computer

If you are using a computer for administration with access to pupil data, you should help protect your computer by locking it when you are away. Locking is different from logging off : when you *log off* your computer, other users can still log on to it. When you *lock* your computer, however, only you or an administrator can log on to it. Open files and running programs are immediately available to you when you unlock the computer and log back on. This could be less important for computers which are used solely for curriculum purposes.

Press CTRL+ALT+DEL and click “Lock Computer” (Your computer can also be locked immediately by pressing the Windows logo key + L.)

To unlock it, press CTRL+ALT+DEL, enter your password, and click OK.)

3. Protect your computer using a screen saver password

A password-protected screen saver offers another layer of protection by preventing others from seeing your screen and using your computer when you are away from it. Whenever the computer is idle for more than a specified length of time, the screen saver starts and the computer automatically locks. When you begin working again you will be prompted to type your password to unlock it. Your screen saver password is the same as your logon password. If you do not use a password to log on, you cannot set a screen saver password.

a) Right-click on the Desktop and click on **Properties**.
b) Under **Screen Saver**, on the **Screen Saver** tab, choose a screen saver from the drop down list.
c) Select the **On resume, password protect** check box.
d) Enter a time delay and click OK.

4. Set up your laptop securely

Although this section specifically covers the setting up of a laptop which is used for school business, it is also important that school computers used for administrative purposes are set up securely. This work will probably be undertaken by the schools ICT technician. Similarly, much of the earlier guidance is also relevant to home users – particularly the guidance on passwords and encryption.

a) You must install Antivirus Software

New worms and viruses are evolving daily and their malicious intent means it is absolutely vital to protect your laptop from infection. They are spreading so fast and in multiple variants that scans for viruses (and spyware) should be carried out daily. The Internet is the main medium for viruses and worms to propagate. Viruses come from the internet via mail attachments and software downloads (especially games, ringtones, etc). Sophos is the recommended antivirus software for schools, and the school licence also covers staff for

computers which they use at home. Your school will have the school username and password you need to use to set Sophos up and further details can be found at : http://www.kirklees-ednet.org.uk/subjects/ictgeneral/technical/sophos.htm

b) It is strongly recommended that you install Antispyware Software

When you visit some web sites on the Internet, you could unknowingly be installing spyware software on your laptop. That spyware software can include trojans or activity tracking software or key logger2 which is automatically installed in your machine. They can perform malicious activity in your laptop, silently monitor your activity and keystrokes and send it to the attacker (e.g. when you login to your bank's internet banking website using secret login ID and password, spyware can track your visited web site's URL and get the secret login ID and password from your key strokes using key logger and send it to the attacker.) Install Anti-Spyware software to protect your computer from spyware. Ad-aware and Spybot are both popular programs which are available free of charge :

Ad-Aware - http://www.lavasoftusa.com/products/ad_aware_free.php
Spybot - http://www.download.com/Spybot-Search-Destroy/3000-8022_4-10122137.html

Notes

- Update anti-spyware software on daily basis.
- Always enable the automatic protection feature of your Anti-Spyware software. This feature will prevent any installation and malicious activity of spyware.
- Scan your laptop regularly (at least once a month) with the Anti-Spyware software.

c) You must set up a Firewall

A firewall reduces surface of attack of your laptop. With a personal firewall, you can minimise the attacks when you are connecting to different networks. Windows XP Professional and Vista come with an inbuilt firewall (see settings below). Older versions of Windows do not have the firewall feature but many firewall software programs are available for download on the internet. The Internet Security Suites are especially useful e.g.

Kaspersky (http://www.kaspersky.com/kaspersky_internet_security)
McAfee (http://uk.mcafee.com/root/package.asp?pkgid=273)
Zone Alarm (http://www.zonelabs.com)
Microsoft Onecare (http://onecare.live.com/standard/en-gb/default.htmv)

To configure personal firewall in Windows XP professional:

1. Right click on **My Network Places** in the Desktop and select **Properties**.
2. Select the **Local Area Connection** or **Wireless Network Connection** icon, right click on it and select **Properties**.
3. In the **Properties** page, go to the **Advanced** tab and enable **Internet Connection Firewall**.
4. Now notice that a padlock icon will come along with the Local area connection icon.

d) You must install Windows Critical Updates

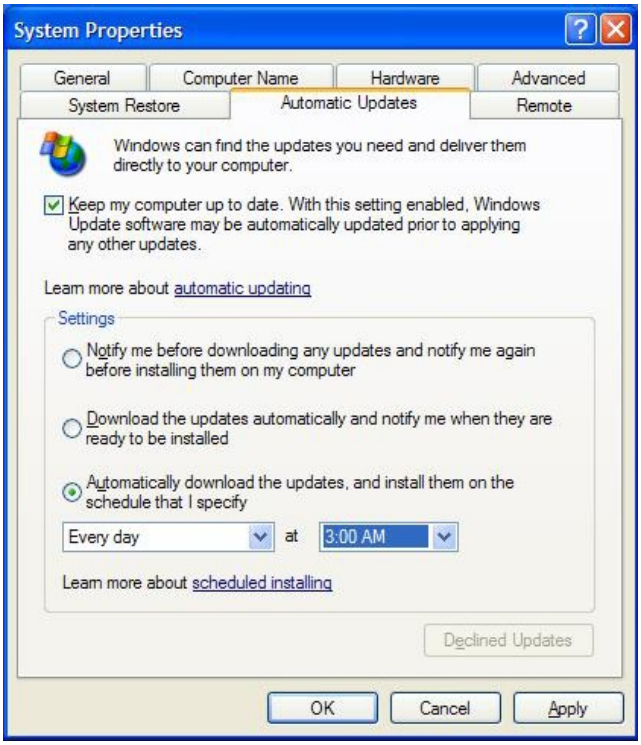
It is important to regularly update Windows with the latest security patches. It can be achieved by using the Windows Update feature. You can manually update Windows easily if you have an internet connection. Type the following URL in your web browser and follow the instructions in the webpage. http://windowsupdate.microsoft.com

If you don't have an internet connection, you can download the patches from the following website to another machine, copy those patches to your laptop and install them manually. http://www.microsoft.com/technet/security/current.aspx

You can also configure Windows to download and install patches in the laptop automatically without your intervention. *(Your laptop must be connected to the internet to perform Automatic Update.)*

To keep your laptop up to date using Windows Automatic Update:

1. Right click on My Computer icon on your desktop.
2. Select Properties from the menu.
3. Select Automatic Updates tab in System Properties page.
4. Check > Keep my computer up to date.
5. Select > Automatically download the updates, choose > Everyday and a convenient time.
6. Click OK.



e) Log onto your laptop with a user name protected by a password

(All school laptops which staff have for their personal use should be set up with different user accounts for home and school (and possibly children). To set up accounts, go to **Start** > **Control Panel** > **User Accounts > Create a new account** – or ask your technician if you don't know how to do this.)

To create a user account password:

1. Click **Start > Control Panel > User Accounts.**
2. Click the account you wish to password protect.
3. Click **Create a Password.**
4. You will then be prompted to enter a password.

When setting user rights for the accounts, it is especially important that children do not have admin user rights!

f) Make sure your Guest account is switched off

The 'Guest' account is another default feature in Windows XP. When the account is enabled anyone may gain access to the laptop in question without a password. While this account only gives limited access to the machine it is the best precaution to make sure the account is switched off.

To switch off the guest account:

1. Click **Start** > **Control Panel** > **User Accounts**
   In the bottom half of the window you will see an icon relating to Guest Account, along with some information telling you whether the account is switched off or switch on. If the account is switched off you need take no action. If the account is switched on, follow the steps below;
2. Click **Guest Account**
3. Click **Turn Off Guest Account**
4. Close the User Accounts Window

g) Configure strong password and account policy settings

(It is recommended that this is only dealt with by a person with technical knowledge.)

By default, the password policy setting in Windows is very weak. You need to protect your account by configuring strong password and account lockout policy, and of course using strong passwords accordingly. Configure the following settings in the account policy of your computer :

To modify the password and account policy:

1. Click **Start** > **Run**, type **secpol.msc** and click **OK**.
2. In the local security settings console, go to
   Security > **Password Policy** or **Account Lockout Policy.**
3. In the right pane of the console, select the policy in question
4. In the properties of the policy, modify the settings
   strong password and account policy settings.

Summary of the required settings:

Password Policy Recommended Security Setting

Enforce password history 5 passwords remembered
Maximum password age 60 days
Minimum password age 0 days
Minimum password length 8 characters
Password must meet complexity requirements Enabled
Store password using reversible encryption Disabled

Account Policy Recommended Security Setting

Account lockout duration 30 minutes
Account lockout threshold 5 invalid login attempts
Reset account lockout counter after 30 minutes

If the computer is running Windows 98, then LM hashes must be removed, otherwise the main Windows password is very weak.

h) Make your files private

Once you have chosen a password you will then be asked if you would like to make you files private. This means that the files you store in your 'My Documents' folder will automatically become private so that only you can read them.
When prompted if you would like to make your files private, **Click Yes**.

To make your folders private (manually) :

- Open My Computer.
- Double-click the C: drive
- Double-click the Documents and Settings folder.
- Double-click your user folder.
- Right-click any folder in your user profile, and then click Properties.
- On the Sharing tab, select the Make this folder private so that only I have access to it check box.

Notes

- This option is only available for folders included in your user profile. Folders in your user profile include My Documents and its subfolders, Desktop, Start Menu, Cookies, and Favorites. If you do not make these folders private, they are available to everyone who uses your computer.
- When you make a folder private, all of its subfolders are private as well. For example, when you make My Documents private, you also make My Music and My Pictures private. When you share a folder, you also share all of its subfolders unless you make them private.
- You cannot make your folders private if your drive is not formatted as NTFS (see below) and there must not be any other users with admin rights (as they can just undo the changes).

i) Do not store any files in the shared folder

By default there is a shared folder in Windows XP. This folder can be seen in 'My Computer'. Any files stored in this folder are automatically shared with anyone and everyone on the network to which you are connected. For this reason you must make sure that you do not store files in this folder unless you wish to share them on your network.

j) Set up secure Internet Explorer settings

Some websites contains dangerous scripts and ActiveX controls. When you visit those websites, scripts are automatically downloaded and executed in your web browser. These malicious scripts can damage your laptop. Protect your laptop from this type of vulnerability by securing the Internet Explorer settings as mentioned below.

To make Internet Explorer more secure :

1. Select **Internet Options** under the **Tools** menu in Internet Explorer browser.
2. Select the **Security** tab and then click **Default Level** and set the slider to **Medium setting**.
3. Select the **Privacy** tab and move the slider to **Medium** setting.
4. Click **Apply** and **OK.**

Specific settings :

- Turn off Autocomplete (for password, filling in forms, etc) (**Internet Explorer > Tools > Internet Options > Content** tab)
- Do not allow Internet Explorer to remember any passwords
- Turn Phishing filter on (in Internet Explorer 7 or MSN toolbar)
- Use the "Always Ask" option before loading Active X scripts
- Use an Internet Security Suite at home as this gives better security than Internet Explorer because settings can locked down with a password more easily to prevent them being changed.
- Remove caching, history, cookies and temporary files (**Internet Explorer > Tools > Internet Options > General** tab)

k) Use only secure NTFS file system

(It is recommended that this is only dealt with by a person with technical knowledge.)

Windows NTFS file system provides file and folder level security. You can protect your important data using NTFS permission so that unauthorised users cannot access it. During the installation of Windows OS, format all the partitions of your laptop using NTFS. If you have existing FAT/FAT32 partition(s) on the laptop, you can convert it to NTFS without destroying your existing data using the Convert command.

To check your current file system format, right click on your local hard drive in 'My Documents' and click Properties. The current file system will be displayed. If your file system is already NTFS, you need take no action.

To convert FAT/FAT32 partition into NTFS:

1. Backup all data of the FAT/FAT32 partition.
2. Click **Start** > **Run**, type **cmd** and click **OK** to open the command prompt.
3. Type the following command: **convert x: /fs:ntfs** (where x is the drive letter)
4. Wait for completion of the conversion process.
5. Reboot the laptop.

l) Disable Bluetooth

Bluetooth is a very insecure method of connecting two devices which should never be used for sharing personal data due to the ease with which it can be intercepted. Also, Bluetooth enables your device to be detected by others which can add a further risk to your security. To disable Bluetooth on your laptop, you will need to check your manual or ask your technician because the method depends on a number of factors such as whether it is built-in or on a USB dongle, and whether the Operating System is Windows XP or Vista. Some laptops use a function key to disable/enable Bluetooth.

A technical solution for Windows XP is available at: http://support.microsoft.com/kb/889814.

It is also advisable to disable Bluetooth on your other devices, such as mobile phones. A short article on Bluetooth security is available at :
http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1085472,00.html

5. Set up your home wireless network securely

a) Set up the network and configure the router with WPA-2 security

Setting up home wireless networks is beyond the scope of this document. There are many books written on the subject and also some excellent guides on the internet. A quick Google search brought up the following useful links :

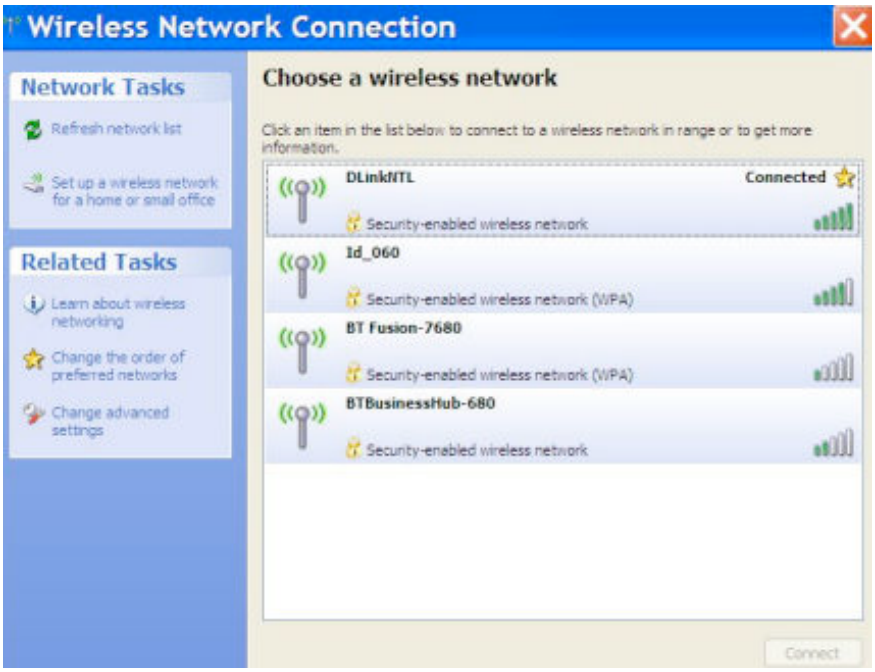
- Microsoft : Set up a wireless network
  http://www.microsoft.com/windowsxp/using/networking/setup/wireless.mspx
  A useful guide which covers the setting up of a wireless network and how to connect Windows XP computers to the network.
- About.com : Wireless / Networking
  http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm
  A very useful site which shows you have to make your home wireless network secure with some very good advice. It has lots of guidance and is clearly explained. Highly recommended.

b) Connect the computer to the network

When your home wireless network has been securely set up, connecting your laptop to the network is relatively straight-forward. The Microsoft web site has the following useful step-by-step guides for connecting computers running Windows XP and Vista :

- Microsoft : Connecting to wireless networks with Windows Vista
  http://technet.microsoft.com/en-us/library/bb878035.aspx
- Microsoft : Connect to a wireless network (in XP)
  http://www.microsoft.com/windowsxp/using/networking/setup/wireless.mspx#4

When connecting your laptop, you will see a screen which lists all the available wireless networks at your location. (Check that the network is security-enabled, if not it will need making secure.)



6. File Encryption

Password protection is insufficient on its own. The most secure systems use a password (or passphrase) to release encryption keys which then decrypt the file so that it can be read.

There are two commonly used file encryption methods : the most secure is Advanced Encryption Standard (AES) encryption, which uses a combination of encryption keys and passwords, and the other, which is probably more commonly used at present is Zip file encryption. Zip encryption is an older technique which is well-supported by a range of third-party software packages. It provides a measure of protection against casual users but it is known to be relatively weak and cannot be expected to provide protection from determined individuals with access to specialised password recovery tools. You should always use AES encryption if possible.

For more information and guidance on file encryption (and information security in general), visit the Open PGP web site : http://www.articsoft.com/info_security.htm

a) AES file encryption

There are many commercial suppliers of AES file encryption software and there is little objective evaluation data, or local experience, with which to compare the different packages. A Google search for “AES encryption software” will provide a list of the major packages, some of which are :

- GNU PGP (http://www.gnupg.org)
- Open PGP Lite (http://www.articsoft.com/open_pgp_personal.htm)
- Winzip (http://www.winzip.com)

b) Zip file encryption

It is important to distinguish between the two features of Zip files : compression and encryption. Simply compressing a file into a .zip file makes it smaller but provides no security at all for the data as any Zip utility can unzip it. So, for security purposes, albeit not very strong, the zip file must also be encrypted.

i) 3rd Party applications

There are several commonly-used third party Zip utility programs, for example :

- Winzip (http://www.winzip.com)
- ZipItFree (http://www.zipitfree.com/)
- 7-Zip (http://www.7-zip.org/)
- Winrar (http://www.rarlab.com)

Notes on Zip encryption safety

- All zip extractors seem to list all the files in the archive before asking for the password so anyone can see the names of the files in the archive without a password.

- If you extract an encrypted file and then delete it in its decrypted form, it may be possible for someone to later "undelete" the file using file recovery software or the Recycle Bin.
- When you open or view a file from an archive (e.g., by double clicking it), the decrypted file is extracted to a temporary location so that the associated program can open it. If you subsequently close the Zip program without first closing the program that is using the file, the Zip program will not be able to delete the temporary copy of the file, thereby leaving it on disk in unencrypted form.
- You may be able to eliminate some of these risks using specialised software, such as disk erasers.

ii) Windows Vista (and XP Professional) - zipped compressed folders

Windows Vista has a built-in system for creating zip files.

1. When creating a new folder from the File menu, point to **New**, and then click **Compressed (zipped) Folder**.
2. Type a name for the new folder and then press ENTER.

Notes

- You can identify compressed folders by the zipper on the folder icon : 
- Files zipped in Windows Vista conform to a standard which can be read by other operating systems.
- If you share compressed folders with users on other computer systems, you may want to limit the compressed folder names to eight characters with a .zip file name extension for greater compatibility.

To protect files in a zipped compressed folder with a password

1. Double-click the compressed folder.
2. On the File menu, click **Add a Password**.
3. In the **Password** box, type a password.
4. In the **Confirm Password** box, type the password again.

Notes

- Passwords are case sensitive.
- If the file is protected with a password, you must provide the password before the file can be extracted to the folder you specify.
- When you extract a file, a compressed version remains in the compressed folder. To delete the compressed version, right-click the file, and then click Delete.
- When you extract a file from a compressed folder that is password protected, the extracted file is no longer protected.

7. Device Encryption (including USB memory sticks)

i) Encrypted volumes (folders or partitions) Truecrypt (http://www.truecrypt.org/)

Truecrypt is a very useful free software solution for encryption. It is well supported with good online guidance including a good beginner's tutorial. It is easy to use after the initial learning phase. A high level of security is provided and it is particularly good for use with USB memory sticks.

The following description is based on information from the Truecrypt web site :

> TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume. On-the-fly encryption means that data is automatically encrypted or decrypted just before it is loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).
>
> TrueCrypt never saves any decrypted data to a disk or USB memory stick. Even when the power supply is suddenly interrupted, without a proper system shut down, files stored in the volume are inaccessible and encrypted. To make them accessible again, you have to mount the volume and provide the correct password and key.
>
> Files can be copied to and from a mounted TrueCrypt volume just like they are copied to/from any normal disk (for example, by simple drag-and-drop operations). Keys can be backed up (it is advisable to do a practice delete and recovery of key.)

Using Truecrypt does add one or two extra steps into loading and saving a file so it is not quite as quick as working with unencrypted files. However, it does ensure that your data is held very securely and if you are currently doing nothing else, Truecrypt is a very good option, especially for USB memory sticks.

Detailed instructions for using Truecrypt are included in the Becta guidance document (see Data Encryption page 40 Encrypting USB Memory Sticks using Truecrypt). Although instructions are also provided for encrypting a whole laptop it is **not** recommended that this is undertaken without Technical support.

ii) Whole device encryption

Device encryption means that the whole computer is encrypted making it unusable by any unauthorised user. Such a solution is not cheap but it provides the highest level of security for our data. InTech have recently completed a procurement process for an encryption system so that Council-owned laptops can be fully encrypted and this service will be available for schools (although there are no details of the likely cost). Contact InTech for further information.

iii) Hardware-encrypted Flash Drives

A number of suppliers now produce USB memory devices with built-in security which sometimes includes fingerprint readers. The devices are more expensive than normal USB memory sticks. Examples include :

- The KanguruDefender is a USB memory stick (available in sizes from 1Gb to 16Gb) which uses 256-bit Hardware AES encryption to secure the whole memory stick. The prices range from £35 ex VAT for the 1Gb version to £250 for the 16Gb version.
- The MXI stealth family - the 1Gb Stealth MXP costs $189 (http://www.mxisecurity.com/?p=products&i=stealth_mxp_family).

iv) Encrypted File System (EFS) feature of Windows XP Professional

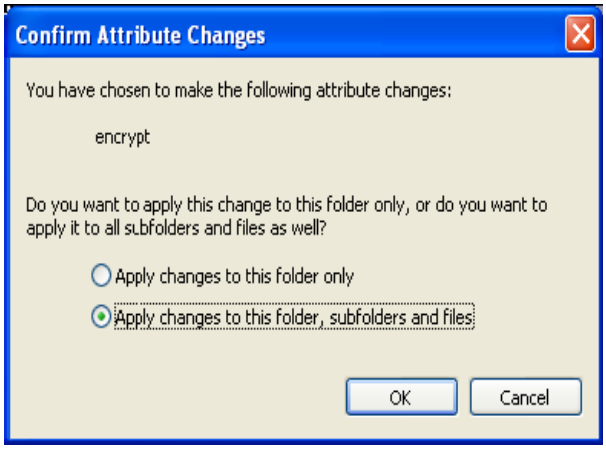
(It is recommended that this is only dealt with by a person with technical knowledge.)

EFS (Encrypted File System) is a powerful security feature of NTFS file system in Windows 2000 and XP Professional that can be used for computers that plug in to a domain but it is a serious undertaking that is difficult to do (**Truecrypt is probably a better solution**). Using this feature you can encrypt and secure your sensitive data. EFS can be implemented at file level and folder level. If you implement EFS at folder level, all files inside the folder will be encrypted using EFS. After encrypting a file or folder using EFS, only you can open it with your login. Unauthorised users will not able to access your data. Even if your laptop is stolen, your sensitive data will be protected.

If your laptop is not on a domain and its' Operating System crashes, then it is not possible to recover encrypted data from the hard disk. Otherwise it is possible, although difficult, to recover using recovery agent account certificate. So before using EFS decide if it meets your requirement, otherwise in the event of a disaster you might not able to recover your data.

To secure your sensitive data using Windows EFS (Encrypted file system):

1. Right click on the **File** or **Folder** in question.
2. Select **Properties** from the menu.
3. In the **General** tab of file or folder properties Click **Advanced** button.
4. In the **Advanced** attributes select **Encrypt contents to secure data**. Click **OK**.
6. If you are encrypting a folder, then in **Confirm attribute changes** dialog select **Apply changes to this folder, sub folder and files** and click **OK**.


Confirm Attribute Changes
You have chosen to make the following attribute changes:
encrypt
Do you want to apply this change to this folder only, or do you want to apply it to all subfolders and files as well?
Apply changes to this folder only
Apply changes to this folder, subfolders and files
OK
Cancel


Advanced Attributes
Choose the options you want for this file.
Archive and Index attributes
File is ready for archiving
For fast searching, allow Indexing Service to index this file
Compress or Encrypt attributes
Compress contents to save disk space
Encrypt contents to secure data
Details
OK
Cancel