Scampton Church of England Primary School
Information and ICT Security Policy and Guidance

Purpose

The objectives of this Policy are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure users are aware of and fully comply with all relevant legislation.
- Ensure staff understand the need for information and ICT security and their own responsibilities in this respect.

At Scampton CE Primary School, teaching staff, support staff and pupils have the expertise and confidence to effectively use ICT on a daily basis to enhance and enrich learning and teaching opportunities.

1 Definitions

"**Information**" means information in any format, eg paper, electronic, video, audio.

"**Authentication**" means the process of identifying an individual, usually based on a username and password, ie determining whether someone is, in fact, who they claim to be.

See Appendix D for definitions for Personal Data and Sensitive Personal Data.

2 Scope

This Policy is intended for all school staff, including governors, who have control over or who use or support the school's administrative and/or curriculum ICT systems or data or handle other school manual (paper) and electronic data.

This policy will be reviewed on a regular basis in line with school priorities. All users of the school's ICT systems or data are also covered by this policy.
Acceptable use policies are also incorporated as appendices to this document.

3 Responsibilities

3.1 The Governing Body

The Governing Body has ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of information and ICT security and for disseminating policy on ICT security and other ICT related matters. In practice, the day to day responsibility for implementing these legislative requirements rests with the Headteacher.

3.2 The Headteacher

The Headteacher is responsible for ensuring that the legislative requirements relating to the use of information and ICT system security are met and that the school's Information and ICT Security Policy, as may be amended from time to time, is adopted and maintained by the school. The Headteacher is also responsible for ensuring that any special security measures relating to the school's information or ICT facilities are applied and documented as an integral part of the Policy.

The Headteacher is also responsible for ensuring the requirements of the Data Protection Act 1998 are complied with fully by the school.

In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy.

Appendix H provides a checklist for headteachers.

3.3 Senior Information Risk Officer (SIRO)

The Senior Information Risk Officer (SIRO) is a senior member of staff who is familiar with information risks and the organisation's response. The following responsibilities attach to the role of SIRO:

- They own the information risk policy and risk assessment
- They appoint the Information Asset Owners (IAOs) – see section 3.4
- They act as an advocate for information risk management

Additionally, the SIRO will be responsible for ensuring that:

- Suitable training for all users and documentation to promote the proper use of information and ICT systems is provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through the school to each individual user will be maintained.

- Users are made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for information and ICT security.

- To help achieve these aims, the relevant parts of the Information and ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

- The SIRO will ensure that the practical aspects of ICT protection are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

In line with these responsibilities, the SIRO will be the official point of contact for ICT or information security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of ICT or information security occurring within the school.

The SIRO or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to the Council's Information Governance team upon request.

The school's Senior Information Risk Officer (SIRO) is Mr Charlie Hebborn

---

3.4 Information Asset Owner (IAO)

Schools must identify their information assets – including personal data for pupils and staff, assessment records, medical information and special educational needs data, for example – and for each one, identify an information asset owner. The role of the IAO is to understand:

- What information is held and for what purposes
- How information has been amended or added to over time
- Who has access to protected data and why

An information asset is regarded as the collection of data or an entire dataset There is an IAO for each asset or group of assets as appropriate.

The IAO is responsible for managing and addressing risks to the information and ensuring that information handling both complies with legal requirements and is used to the full to support the delivery of education.

The school's Information Asset Owners are:
Charlie Hebborn – Headteacher - Pupil Performance Data, Staff performance data, Child Protection Information, SEN information
Tracy Wickens – SIMs Pupil information/ Medical

3.5 Audit Services

The Audit Services section of the Council is responsible for checking periodically that the measures prescribed in each school's approved Information and ICT Security Policy are complied with, and for investigating any suspected or actual breaches of ICT or information security.

3.6 Users

All users of the school's ICT systems and data must comply with the requirements of the School's Information and ICT Security Policy.

Users are responsible for notifying the SIRO of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Audit Services.

Although the above roles have been explicitly identified, the handling of secured data is everyone's responsibility.

4 Legislation

4.1 Background

The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems and information security, which comprise principally of:

- Data Protection Acts1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Human Rights Act 1998

It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

The general requirements arising from these Acts are noted in Appendix B

5 Management of the Policy

The Headteacher should allocate sufficient resources each year to ensure the security of the school's information and ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors.

The Headteacher must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied to provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:

- a record that new staff have been issued with, have read the appropriate documentation relating to information and ICT security, and have signed the list of rules;
- a record of the access rights to systems granted to an individual user;
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.

6 Physical Security

6.1 Location Access

Adequate consideration should be given to the physical security of rooms containing sensitive information and ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.

The SIRO must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

All school owned ICT equipment should be recorded in the school asset register.

Power supply protection from voltage surges will prevent servers from failing. Uninterruptible Power Supply (UPS) units will ensure a controlled shutdown of servers should a power failure occur. Uninterruptible Power Supply units are also recommended for network cabinets which contain sensitive equipment, ie Cisco network switches.

6.2 Siting of Equipment

Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- Information (paper or electronic) should be protected in such a way that it cannot be accessed or viewed by persons not authorised to access it.
- devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- equipment should be sited to avoid environmental damage from causes such as dust and heat;
- users should enable password protected screen savers to protect screen content if unauthorised access to the data held can be gained when left unattended
- a ‘clear desk policy’ should be adopted, ie hard copies of sensitive data are not left unattended on desks;
- network servers and infrastructure should be located in a temperature controlled, secure environment. If temperature control is not feasible, then the room should be well ventilated.

The same rules apply to official equipment in use at a user’s home.

Storage and access to paper/manual information should be sited in such a way.

Physical Security – Checklist

	Set up password protected screen savers for staff access
	Adopt a clear desk policy
	Position computer screen so that information displayed cannot be read by an unauthorised person
	Ensure server rooms are secure and well ventilated
	Sensitive or personal information should not be left on a computer screen whilst a teacher is away from the PC
	Sensitive or personal information should not be projected in a classroom environment

7 Inventory

The SIRO, in accordance with the School's Financial Regulations, shall ensure that an inventory of all ICT equipment (however financed) is maintained and all items accounted for at least annually.

A current and up to date software inventory should also be maintained.

7.1 Personal Hardware and Software

Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all personal hardware and software for school purposes must be approved by the SIRO.

Many free to use pieces of software may require payment for business use. The SIRO must be satisfied that use is permitted or paid for where required.

Inventory – Checklist

	Keep an up to date hardware inventory
	Keep an up to date software inventory
	Keep a record of equipment disposals

8 System Security

Any contractors or third parties who require access to the school's ICT systems for support or other reasons, should sign the agreement "Access to Systems and Facilities by Contractors" before access is granted. See Appendix A for guidance notes for adults working with young people.

8.1 Legitimate Use

The school's ICT facilities must not be used in any way that breaks the law or breaches Council standards (see also LCC fair usage policy).

Such breaches include, but are not limited to:

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorised private use of the school's computer facilities.

8.2 ICT Security Facilities

The school's ICT systems and data will be protected using appropriate security arrangements outlined below. In addition consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.

Administrative and curriculum network traffic is separated by the use of virtual LANs (Vlans) across the broadband network.

If Wireless LANs are implemented, they must be configured for encryption of network traffic and with no broadcast to prevent unauthorized access to school data. Encryption passwords should be stored securely by the SIRO. Administrative PCs should not be accessible via wireless networking unless there is an approved managed wireless solution in place providing authenticated access to secure data.

8.3 Authorisation

Only persons authorised by the SIRO, are allowed to use the school's ICT systems. The authority given to use a system will be sufficient but not excessive and the authority given must not be exceeded.

Failure to establish the limits of any authorisation may result in the school being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.

All ICT systems should display a message to users warning against unauthorised use of the system.

Access eligibility will be reviewed continually, including remote access to systems and external web services, eg S2S, Lincolnshire Data Exchange. In particular the

relevant access capability will be removed when a person leaves the employment of the school or their role changes. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.

Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

SeeAppendix E "Checklist for Leavers" document

8.4 Access to the Council Services

The SIRO must seek permission on behalf of the school for any ICT user to access Council services.

8.5 Passwords

Passwords protect access to ICT systems.

All accounts with "administrator" rights should have strong passwords. The recommendation for strong passwords is a minimum of 16 characters, using a combination of upper and lower case, numbers and symbols

The level of password control will be defined by the SIRO based on the value and sensitivity of the data involved, including the possible use of "time out" passwords where a device is left unused for a defined period.

Power on passwords are recommended for mobile devices, particularly laptops highly portable and less physically secure.

Default passwords must be changed the first time a system is used.

Passwords should be memorised. If an infrequently used password needs to be written, this record must be stored securely. Users should be advised about the potential risks of written passwords and should be given clear written instructions on the safeguards to adopt.

Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data involved, ie 'master user' passwords are more critical. Users should be instructed on appropriate techniques for selecting and setting a new password. Passwords are to be changed on a termly basis.

A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:

- when a password holder leaves the school or is transferred to another post;
- when a password may have become known to a person not entitled to know it.

The need to change one or more passwords will be determined by the risk of the security breach.

Users must not reveal their password to anyone. Users who forget their password must request the SIRO issue a new password.

Where a password has to be shared, eg to power on a device or access an internal network, users must take special care to ensure that it is not disclosed to any person who does not require access to the device or network.

8.6 Backups

The school uses Google Apps for Education which provides ‘cloud back up’ which is password protected for each user.

The ‘W’ Drive contains more sensitive information that can be accessed by the administrator and the Headteacher only. This information is securely stored on the school’s server and the back up drive.

8.7 Virus Protection

The SIRO will ensure current and up to date anti-virus software is applied to all school ICT systems.

The SIRO will ensure operating systems are updated with critical security patches as soon as these are available and ensure that there is a mechanism in place for ensuring that there is a mechanism for keeping all operating systems up to date.

The SIRO will ensure that where personal equipment, eg pupil or staff owned PDA, laptop, is brought into school, there is a clear policy regarding the minimum security measures required before the connection of such devices to the school network.

It is the school’s responsibility to ensure that all school owned equipment is managed so that anti virus and critical security updates are applied in a timely manner.

All users take precautions to avoid malicious software that may destroy or corrupt data, eg checking all incoming email attachments or internet downloads for malicious software before use, and should be made aware of how to recognise and handle email hoaxes.

The school will ensure that every ICT user is aware that any suspected or actual computer virus infection must be reported immediately to the SIRO who must take appropriate action, including removing the source of infection.

8.8 Disposal of Information and Equipment

Disposal of waste information and ICT media such as print-outs, CDs, memory sticks and magnetic tape will be carried out in a secure manner to ensure that the information contained cannot be recovered or reconstructed. For example, paper and CDs will be shredded if any confidential information from them could be derived.

The Data Protection Act requires that personal information is disposed of securely.

Prior to the transfer or disposal of any ICT equipment the SIRO must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met.

It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

The SIRO must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

8.9 Repair of Equipment

If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on other media for subsequent reinstallation.

System Security – Checklist

	Ensure any contractor or third party signs the form “Access to Systems by Third Parties” before access is granted
	Establish Acceptable Use Policies and ensure that these are issued to all users
	Set rules governing the use of private hardware and software
	Ensure access granted to users is sufficient
	Establish a leavers’ procedure to ensure that accounts are deleted when users leave
	Enforce strong passwords where appropriate
	Ensure all school owned machines are managed so that AV and critical security updates are applied in a timely manner
	Ensure disposal is carried out in a secure manner as appropriate and that equipment disposals are recorded

9 Good Practice in Information Handling

9.1 Background

Good practice guides to support schools in reviewing their data handling procedures are available:

- Information risk management and protective marking
- Secure remote access
- Data Encryption
- Audit logging and incident handling

Every school holds personal data on learners, staff and others. Information security is everyone's responsibility and needs to be embedded into the culture and ways of working.

Personal data is any combination of data items that identifies an individual and gives specific information about them, their families or their circumstances. This includes names, contact details, gender, dates of birth, behavior and assessment records. The Data Protection Act 1998 specifies additional data items as "sensitive personal data" including medical records, criminal convictions and ethnic origin.

9.2 Risk Assessment

It is recommended that every school undertakes a thorough risk assessment on the information assets held. This will help identify what security measures are already in place and whether they are the most appropriate (and cost effective) available. Carrying out an information risk assessment will generally involve:

- Recognizing which risks are present
- Judging the size of the risk(s)
- Prioritising the risks

Once the risks have been assessed, a decision can be made on how to reduce them or accept them.

Risk assessment is an ongoing process and schools will need to review these at regular intervals as risks change over time.

9.3 Encryption

Schools should use encryption to help maintain the security of the personal data they hold on learners, staff and others and if sensitive or personal information is held on a mobile device, then this must be encrypted.

Data Handling – Checklist

	Appoint a Senior Risk Information Officer (SIRO)
	Identify information assets and for each one, identify an Information Asset Owner (IAO)

	Conduct data security training for all users
	Put in place a policy for reporting, managing and recovering from incidents which put information at risk
	Shred, pulp or incinerate paper when no longer required
	Make staff and learners (and parents where applicable) aware of what data is being held about them and what it is being used for by issuing privacy or fair processing notices
	Encrypt media that contains personal data that is to be removed from site or from the organization
	Make sure that, where appropriate, contracts for employment state that misuse of such data is a disciplinary matter

10 Security Incidents

All suspected or actual breaches of information or ICT security, including the detection of computer viruses, must be reported to the SIRO who should report the incident to the appropriate body.

Security Incidents – Checklist

	If you suspect a computer has been used inappropriately, do not turn off or allow anyone to access the computer as it may affect importance evidence
	Make sure all suspected or actual security breaches are reported

Appendix A

E-safety – Sample Acceptable Use Policies for Schools

AUP Guidance notes for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

AUP Guidance notes for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me
- never agree to meet a stranger

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

AUP Guidelines for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

Please check that this is compatible with your local authority policies before using this AUP.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Continued…

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - pornography (including child pornography)
    - promoting discrimination of any kind
    - promoting violence or bullying
    - promoting racial or religious hatred
    - promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to online dangers
- forward any information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or his/her delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

Please check that this is compatible with your local authority policies before using this AUP.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed a Safeguarding Governor with responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix B

Legislation

Data Protection Act 1998

A school, like every other data user, must conform to the requirements of the Data Protection Act (1998). In particular this requires the school to formally notify the Information Commissioner of:

- the purposes for which the school holds personal data;
- what data it holds;
- the source of the data;
- to whom the data is disclosed.

Under the Act, each school is a separate data user and must complete a "Notification" each year.

It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

Computer Misuse Act 1990

Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:

- unauthorised access to a computer system or data;
- unauthorised access preparatory to another criminal action;
- unauthorised modification of a computer system or data.

Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or license.

All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective license or contract.

The School is responsible for compiling and maintaining an inventory of all software held, including freeware and shareware, and for checking it at least annually to ensure that software licenses accord with installations. To ensure that the school complies with the Copyright, Designs and Patents Act 1988 users must get prior permission in writing from their SIRO (or nominated person) before copying any software.

Freeware or shareware software should be registered as required with the software supplier and is generally provided on an unsupported basis. Schools need to be extremely cautious in accepting free downloadable software over the internet. Very

often free software also loads malware software onto the PC. Malware resides and hides on computers, often reporting back to advertising companies or other data capture firms that build up a profile of internet browsing habits.

Users should read all licence agreements very carefully before accepting the terms and conditions and, if in any doubt, should not accept the licence conditions/download.

All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

Freedom of Information
The Freedom of Information Act (FOI) came into force on 1st January 2005. This means that members of the public and organisations have rights of access to information held by public bodies. Upon request we must tell individuals if we hold information and if so, provide it within 20 working days.

The principle behind the Act is that all information held in any format is accessible, unless certain conditions or exemptions apply.

Further information on the Act and the application of exemptions is available on SchoolsNet/Learning Gateway.

If an individual is not satisfied with our response, or if we do not respond within the 20 working days, they can request a review of the request. If they are not satisfied with the review process they can make a complaint to the Information Commissioner's Office.

A request can be given to any employee of the Council. Once a request is received you need to know what to do with it and act upon it immediately. All staff will need to make sure they know how the procedures affect them.

Human Rights
As a public authority, the school must act in a way that is compatible with and promotes individuals' rights in accordance with the Human Rights Act 1998.

Further information is available via the following weblink:
http://www.justice.gov.uk/guidance/humanrights.htm

Definitions
Definitions of Personal Information and Sensitive Personal Information for this purpose are:-

Personal data: Information that is sufficient to identify a living individual by itself or in conjunction with other information held by the school. Includes any expression of opinion about an individual and any indication of the intentions of the school or any other person in respect of the individual.

Sensitive personal data: Defined in the Data Protection Act 1998 as information about an individual relating to physical/mental health, criminal proceedings, ethnicity, sexual life, trade union, political opinions or religious beliefs.

Other data that should be protected includes: national insurance number, bank account details, credit card details, identification credentials and protected whereabouts.

Appendix C

Secure Remote Access

Schools should use secure remote access technology, where appropriate, to secure the personal data of learners, staff or any other authorised users.

Essential components of secure remote access include:

- Authentication – who or what system is trying to connect, ensuring that the user and the computer at each end are who they say they are
- Authorisation – ensuring that the user at the remote end is authorized to access the data
- Geographical restrictions – personal data may not be access remotely unless encrypted and access may require specific network connections
- Encryption – to secure personal data in transit, and file or full disk encryption for any storage media that holds personal data
- Audit – logs of access to secured data

Appendix D

E-Mail

Recommendations for email users:

- Ensure you have read the Acceptable Use Policy
- Report any spam or phishing emails to the appropriate contact in your school, eg SIRO, ICT co-ordinator, network manager
- If you don’t know the sender of an unsolicited email, delete it without opening it
- Don’t click on links in unsolicited emails and be especially wary of emails requesting or asking confirmation of any personal information, such as passwords, bank details etc
- Don’t turn off any email security measures that your school has implemented or recommended
- Never respond to any spam message or click on any links in the message
- Don't use the preview function for your Inbox
- When sending email messages to a large number of recipients, use the blind copy (BCC) field to conceal their email addresses
- Think carefully before providing your email address on websites, newsgroup lists or other online public forum
- Never give your primary email address to anyone or any site you don't trust
- Do not take part in email chain letters
- Do not include indecent, inappropriate, offensive or profane content in any email

Appendix E

LEAVERS– CHECKLIST FOR MANAGERS

Please refer to this checklist as appropriate. If you are uncertain about any aspects of the checklist or require further explanation, please contact the SIRO. Please note it is your responsibility to ensure that the items below are returned as detailed.

Employee Name		Employee No	
School		Post No	
Post Title		Leaving Date	

Please ensure return of:	**Tick**	**Initials**
ID/Security Badge returned	Yes ☐ No ☐ N/A ☐	
Uniform/Protective Clothing	Yes ☐ No ☐ N/A ☐	
School Property (keys, personal alarm etc)	Yes ☐ No ☐ N/A ☐	
School data (paper files, CDs, removable media etc	Yes ☐ No ☐ N/A ☐	
School hardware (laptop, PC, mobile phone, memory stick etc)	Yes ☐ No ☐ N/A ☐	
Service/contract considerations	**Tick**	**Initials**
Alarm/door system – is code change required?	Yes ☐ No ☐ N/A ☐	
Key Holder – consider new arrangements?	Yes ☐ No ☐ N/A ☐	
Alert contractors to new contact arrangements?	Yes ☐ No ☐ N/A ☐	
Consider First Aid / Fire Warden requirements?	Yes ☐ No ☐ N/A ☐	
IT considerations	**Tick**	**Initials**
SIMS database amended	Yes ☐ No ☐ N/A ☐	
Email account(s) disabled	Yes ☐ No ☐ N/A ☐	
Active Directory Account disabled	Yes ☐ No ☐ N/A ☐	
Access to external websites disabled (SLG, S2S etc)	Yes ☐ No ☐ N/A ☐	

Appendix F

Appendix G

Sample Record of Asset Disposal Form

Record of Asset Disposal

School:

I hereby authorise the disposal of the items detailed below for the net value shown (where appropriate):

Inventory Ref:	**Description of Items**	**£**

Method of Disposal: Sale / Transfer / Discarded (Damaged / Obsolete) (delete as appropriate)

Details of Sale / Transfer

Has the Inventory been amended? Yes /No

Name of Certifying Officer

Signature

Date

Appendix H

Checklist

This checklist is designed to assist Headteachers ensure that personal information in either paper or electronic format is being managed appropriately.

It is the Headteacher's responsibility to:

- know how personal information is being used.
- approve what personal information leaves the school premises.
- ensure that staff are taking precautions to ensure that personal information is approriately protected.

Checklist	
Check with staff if they take personal information or equipment away from school.	☐
Does personal information need to be taken off site?	☐
Is the amount of personal information leaving the school limited to that which is actually needed, ie data isn't left on memory sticks or laptops if it is not specifically required?	☐
Personal data isn't stored on memory sticks or laptops unless the devices are encrypted. The Information Commissioner's Office does not consider password only protection to be sufficient.	☐
When taken out of the school, personal information is going to be kept securely and access limited to the member of staff, either in transit or in the home environment.	☐
Is anti-virus software and operating system software (Windows/Mac) kept up to date? At a minimum staff must ensure that laptops are updated as soon as they are returned to school. [The Council has previously suffered a serious incident affecting the whole school network as a result of computer software not being kept up to date over a Summer break].	☐
If school computer equipment is being taken home, access to the computer is restricted to the member of staff's usage.	☐
Personal photographs, music, video, non-school software should not be stored on a school computer.	☐
Staff are aware that they should use the computer in the home environment as they would at school, in line with any school 'appropriate usage' guidance.	☐
When the school is closed personal information and portable computer equipment remaining at school is secured out of sight.	☐

Examples of school related data breaches:

School memory stick breach:
http://www.ico.gov.uk/upload/documents/library/data_protection/notices/st_james_primary_school_undertaking.pdf

School Admin Computer Theft:
http://www.ico.gov.uk/upload/documents/library/data_protection/notices/ysgol_bro_famau_undertaking.pdf

Theft of school laptop:
http://www.ico.gov.uk/upload/documents/library/data_protection/notices/waseley_hills_high_school_undertaking.pdf