

CHURCH STRETTON SCHOOL



Information and ICT Security Policy

Updated May 2011

Due for review July 2012

Senior Information Risk Owner (SIRO) P. Tilson

I:drive/Policies/Information and ICT Security

Status

Date established by the Governing Body...

June 2011

Date for full implementation

September 2011

Date for Review

July 2012

Senior Information Risk Officer

P. Tilson

The policy is available for staff at:

Staff room, Department Handbook, Learning Gateway

Church Stretton School has made a significant investment in computer systems and networks. Reliable ICT services are vital to teaching, learning and management tasks. In addition, the school manages a wide range of personal and sensitive information.

The school has access to the Shropshire wide area network (WAN), providing them with access to corporate resources such as Samis and ResourceLink.

We recognise that this wider access places a responsibility on us to ensure that our own local area network and the Shropshire WAN, as well as the personal information they manage, is not compromised by poor security and irresponsible user actions.

Objectives

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 all staff understand the need for information and ICT security and their own responsibilities in this respect.

Consultation

This policy has been developed in liaison with:

- Network manager
- Head of ICT
- Senior Leader ICT link
- Headteacher

Relationship with other policies

This policy relates to the following whole school policies and documents:

- Acceptable use Agreements for staff and pupils
- Laptop computers for Staff policy
- Laptop computers for Students policy
- Safeguarding policies
- E – Safety policy and statements
- Curriculum ICT policies and handbook

Arrangements for monitoring and evaluation

This policy will be reviewed annually and will be approved by the Health and Safety committee of the Governing Body.

Policy Definitions

“**Information**” means information in any format, e.g. paper, electronic, video, audio.

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

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

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.

All users of the school's ICT systems or data are also covered by this policy.

Responsibilities

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. Key Legislation is outlined in appendix E. A checklist for governors is included in appendix C

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 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 I provides a checklist for Headteachers.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is a senior member of staff who is familiar with information risks and the school'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)
- 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.
- 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.
- The SIRO has a responsibility for ICT equipment and systems and will have control over these assets and their use, including responsibility for controlling access to these assets and for defining and recording the requisite level of protection.

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 SIRO or Chair of Governors must advise the ICT Services Help Desk (01743) 252200 of any suspected or actual breach of ICT or information security immediately.

It is vital, therefore, that the SIRO is fully conversant with the Information and ICT Security Policy and maintains an up to date knowledge of best practice and follows the associated approved practices.

*The school's Senior Information Risk Officer (SIRO) is Mr **Paul Tilson***

Information Asset Owner (IAO)

The School has identified its information assets – including personal information and data regarding pupils and staff, assessment records, medical information and special educational needs data, for example. For each data asset we have identified 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

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:

- | | |
|--|---------------------------|
| • SIMS data and pupil records | Mrs C Floyd / Mr P Tilson |
| • SEN data, records and documentation | Mr J Smith – SENCO |
| • Centrally held Assessment and tracking information | Mrs D Lowther |
| • Examination data including entries, grades and marks | Mrs H Merrett |
| • Pupil Library information | Mrs S Fletcher |
| • Finance and personnel / payroll information | Mrs C Thomas |
| • Child protection files and information | Mr P Tilson |
| • Extended services (CHAT, student support) | Mrs D Lowther |
| • Behaviour reports and logs | Mr J Parr / Mr J Smith |

Audit Services

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

We will seek specialist advice and information on ICT security as needed from IT Support Service (SITSS), or the Council's Information Governance team.

Users

All users of the school's ICT systems and data must comply with the requirements of our Information and ICT Security Policy. The handling and management of secured data is everyone's responsibility.

Acceptable Use Policies are included in appendices A, B, D and F

Users are responsible for notifying the SIRO of any suspected or actual breach of ICT security. Where this is not possible notifications should be made direct to the Head or to the Chair of Governors.

Legislation

The School recognises the requirements of the current legislation relating to the use of ICT systems and information security, which comprise principally of:

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

Through briefings and training all staff will be kept 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 in the appendices to this document – see page 31.

Management of the Policy

The Headteacher will allocate sufficient resources each year to ensure the security of the school's information and ICT systems and to enable all 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.

Measures are in place to provide for continuity of ICT security when staff vacate or occupy a post. We will maintain:

- 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.

Physical Security

Location Access

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

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

All school owned ICT equipment will be recorded and security-marked. Where appropriate we will seek advice from Shropshire Council's Crime Prevention Officer as to best practice in this area.

Where necessary we will use Power supply protection from voltage surges to minimize the risk of servers failing. Uninterruptible Power Supply (UPS) units are used to ensure a controlled shutdown of servers and network cabinets should a power failure occur.

Siting of Equipment

All staff will be made aware that 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, i.e. hard copies of sensitive data are not left unattended on desks;
- network servers and infrastructure are to be located in a temperature controlled, secure environment. If temperature control is not feasible, then the room should be well ventilated.

These rules will also apply to school equipment in use at a user’s home.

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

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. Records will be kept of all assets disposed of and the measures taken to ensure protection of sensitive data.

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 or, where appropriate, the Network Manager.

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

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 G)

All staff will be made aware of the guidance notes for adults working with young people. (See appendix B)

Legitimate Use

The school's ICT facilities must not be used in any way that breaks the law or breaches Council standards.

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.

ICT Security Facilities

The school's ICT systems and data will be protected using appropriate security arrangements outlined below. In addition consideration will 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. Where we wish to allow cross network traffic we will ensure that there are adequate security measures in place to preserve the confidentiality, integrity and availability of sensitive data.

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

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.

We note that 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, e.g. S2S. 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.
(See appendix F)

Access to the Council Services

The SIRO will seek permission on behalf of the school for any ICT user to access Council services. This will include the Council's SAMIS finance system.

Passwords

Passwords protect access to ICT systems.

All accounts with "administrator" rights should have strong passwords. These should be alpha-numeric and include upper and lowercase letters and symbols. Whilst an 8 character password may be deemed sufficient in some instances, the SIRO may insist on 16 characters for access to particularly sensitive information i.e. "master user" passwords are more critical.

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 and other devices which are 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 be changed frequently to previously unused passwords. The SIRO should decide on the appropriate duration that users could leave their password unchanged.

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 or Network Manager issue a new password.

Where a password has to be shared, e.g. 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.

Users are discouraged from saving passwords in any sort of web browser log on page.

Backups

In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, backup copies of stored data will be taken at regular intervals as determined by the SIRO, dependent upon the importance and quantity of the data concerned.

Security copies should be clearly marked as to what they are and when they were taken and stored away from the system to which they relate in a restricted access fireproof location and/or off site.

Security copies should be regularly tested to ensure that they enable the systems/relevant file to be reloaded in cases of system failure.

Virus Protection

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

The Network Manager 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, e.g. pupil or staff owned PDA, laptop, is brought into school, there is a clear protocol regarding the minimum security measures required before the connection of such devices to the school network.

All users should take precautions to avoid malicious software that may destroy or corrupt data, e.g. 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. In the event of SITSS notifying the school of a virus infection on the school network, the machine(s) must be disconnected immediately and appropriate action taken before reconnection.

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 authorized 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.

A draft Disposal of Asset Form is given in appendix H

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. The Council's Procurement Framework will be utilized where necessary to dispose of redundant equipment in accordance with the WEEE directive.

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.
✓	Acceptable Use Policies in place and issued to all users
✓	Clearly set rules governing the use of private hardware and software
✓	Ensure access granted to users is sufficient
✓	Established leavers' procedure to ensure that accounts are deleted when users leave
✓	Enforce the use of strong passwords where appropriate
✓	All school owned machines are managed so that AV and critical security updates are applied in a timely manner
✓	Disposal is carried out in a secure manner as appropriate and equipment disposals are recorded

Good Practice in Information Handling

Background

Following a number of high profile personal data losses from government departments, policies have been issued aimed at putting in place core protective measures, getting the working culture right and improving accountability and scrutiny of performance. In addition, the Information Commissioner has the power to fine organizations up to £0.5 million for personal data loss.

Church Stretton School makes use of good practice guides to support our review of data handling procedures. These include:

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

Information security is everyone's responsibility and needs to be embedded into our 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.

Risk Assessment

As recommended, the SIRO undertakes a thorough risk assessment on the information assets held. This helps to 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 the schools will review these at regular intervals as risks change over time.

Encryption

When appropriate the School will use encryption to help maintain the security of the personal data held 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

Security Incidents

All suspected or actual breaches of information or ICT security, including the detection of computer viruses, must be reported to the SIRO and the Network Manager, or the Headteacher in their absence, who should report the incident to the ICT Services Help Desk (01743 252200).

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

DRAFT Guidance notes for learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- set strong passwords which I will not share
- not use my own mobile device in school unless I am given permission
- respect copyright and the intellectual property rights of others
- only create and share content that is legal
- always follow the terms and conditions when using a site
- only visit sites which are appropriate
- discuss and agree my use of a social networking site with a responsible adult before joining
- obtain permission from a teacher before I order online
- only use approved email accounts
- only use appropriate content which I have permission to use
- only communicate online with trusted users
- never meet an online friend without taking a responsible adult that I know with me
- make sure all messages/posts I send are respectful
- not respond to or forward any inappropriate message or content
- be cautious when sharing personal contact information
- only communicate electronically with people I know or have been approved by my school
- report unsuitable content or activities to a member of staff

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.

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



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 children in my care to danger
- any other information which may be offensive to others
- forward chain letters
- breach copyright law
- do anything which exposes others to danger

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.

Appendix B

DRAFT Guidelines for any adult working with learners

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

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 (e.g. Face- book, 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 danger
 - any other 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 SIRO or their 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 AUP 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.

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 an e-Safety Coordinator and a named governor takes 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

DRAFT Acceptable Use Policy for Parents and Carers (Online Reporting)

Introduction

Church Stretton School provides parental/carer access to information held about their child in the school's database system (referred to below as "the system"). The information is provided on a read-only basis and cannot be changed by the viewer. Information is provided on the following areas:

- Attendance and
- behaviour Progress and
- attainment Special needs

Security

Access to the system is through the use of a username and password provided by the school to you on an individual basis. It is your responsibility to keep the username and password confidential and to ensure it is not disclosed to any other person.

Please remember that you are responsible for protecting the data you are using from access by any third party.

This policy is intended to minimise security risks. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials
- The wrongful disclosure of private, sensitive and confidential information.
- Data used in such a way which may bring the school or Council into disrepute

Authorised Users

- Access to the system is provided for use by persons who are legally responsible for pupil(s) currently attending the school.
- Access is granted only on condition that the individual formally agrees to the terms of this policy by signing and dating the policy.
- An authorising member of school staff will confirm that there is a legitimate entitlement to access information
- A copy of this form will be held by the school for audit purposes.

Personal Use

Information made available via the system is confidential and protected by law under the Data Protection Act 1998. To that aim:

- Users must not distribute or disclose any information obtained from the system.
- Users must ensure that, when working from home, other family members and friends cannot access the information
- Users should not attempt to access the system in any environment where the security of the information may be placed at risk e.g. a cybercafé or by using an unsecured wi-fi connection.
- All passwords must be kept confidential
- Any errors or inaccuracies in the data viewed should be notified to the school so that appropriate action can be taken

Password Policy

You assume personal responsibility for your username and password.

The password can be changed as necessary in order to maintain security.

(New passwords should be at least 8 characters long and contain a lowercase letter, and uppercase letter and a number or special character.

Cancellation of access

The school reserves the right to revoke or deny access to the system for any individual in the following circumstances:

- The validity of parental responsibility is questioned.
- Court ruling preventing access to child or family members is issued.
- A user is found to be in breach of this policy.
- Any other reason deemed appropriate by the Senior Information Risk Officer, Headteacher or Chair of Governors

A username and password will not be issued unless the attached confirmation is signed and returned to the school

I accept the terms of this policy and request the issue of a username and password:

Parent/Carer of (pupil
name):

1

Tutor Group:

2.

3.

Signed

Please Print Name

Date

Email
address

Appendix E

Key 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.
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. This 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 F

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, e.g. SIRO, ICT co-coordinator, 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 F

LEAVERS – CHECKLIST FOR MANAGERS

Please complete this checklist as appropriate, ensuring it is signed, dated and returned to the SIRO for audit purposes. 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 <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Uniform/Protective Clothing	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
School Property (keys, personal alarm etc)	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
School data (paper files, CDs, removable media etc)	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
School hardware (laptop, PC, mobile phone, memory stick etc)	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Service/contract considerations	Tick	Initials
Alarm/door system – is code change required?	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Key Holder – consider new arrangements?	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Alert contractors to new contact arrangements?	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Consider First Aid / Fire Warden requirements?	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
IT considerations	Tick	Initials
SIMS database amended	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Email account(s) disabled	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Active Directory Account disabled	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	
Access to external websites disabled (SLG, S2S etc)	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>	

This declaration is to be signed by the employee and line manager to confirm that all school equipment and information has been returned or destroyed as appropriate. Please understand that the school will seek to recover any claims/damages made against them as a result of inappropriate use of information.

The employee confirms that all personal information has been removed and all business information transferred from the employee's email account(s) and computer network folder(s).

Employee signature		Manager signature	
Employee name		Manager name	
Date		Date	

Appendix G

Access to Systems or Facilities by Contractors

This agreement should be signed by all contractors accessing Council systems or facilities prior to access being granted.

By signing this form you are agreeing:

- to comply with the Council's Information Security Policy and procedures and take all necessary steps to ensure the security integrity and confidentiality of all data and other information held by the Council to which you shall have access
- to conform with the provisions of all relevant legislation inclusive of but not limited to the Data Protection Act 1998, Copyright Designs and Patents Act 1988, Computer Misuse Act 1990 and all subsequent relevant legislation
- that you will not without the prior consent of the Council in writing divulge data or any other information provided to you by the Council or held by the Council to which you shall have access
- that you will take all reasonable precautions to ensure that viruses or other malicious software are not introduced onto or into the Council's IT facilities or systems
- that you will not without the previous consent of the Council in writing make any change or alteration to IT facilities or systems used by the Council
- that you will not access any of the Council's data information systems or facilities unless it is required to do so under the terms of the Contract and in any event not without the Council's prior consent in writing. This includes only accessing information or systems specified by the Council and in accordance with agreed times of access.
- will not disclose methods of access to facilities or systems to any person without the Council's prior consent in writing
- will not download the Council's accessed data or other information without the Council's prior consent in writing

The Contractor shall fully indemnify Shropshire County Council against all damages (excluding consequential damages), costs, charges and expenses arising from or incurred by its failure to comply with the above clauses and shall promptly notify Shropshire County Council in writing of any alleged infringement of which the Contractor has notice of. The Contractor will make no admissions of liability without Shropshire County Council's prior written consent. The provisions of this Clause shall survive the expiration or termination of this or any related Agreement.

Please sign below to acknowledge that you have read and understood this document and agree to the conditions therein.

Signed:

Name:

Date:

Organisation:

Draft 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

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 appropriately protected.

Headteacher / SIRO checklist	
Check with staff if they take personal information or equipment away from school.	<input type="checkbox"/>
Does personal information need to be taken off site?	<input type="checkbox"/>
Is the amount of personal information leaving the school limited to that which is actually needed, i.e. data isn't left on memory sticks or laptops if it is not specifically required?	<input type="checkbox"/>
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.	<input type="checkbox"/>
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.	<input type="checkbox"/>
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].	<input type="checkbox"/>
If school computer equipment is being taken home, access to the computer is restricted to the member of staff's usage.	<input type="checkbox"/>
Personal photographs, music, video, non-school software should not be stored on a school computer.	<input type="checkbox"/>
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.	<input type="checkbox"/>
When the school is closed personal information and portable computer equipment remaining at school is secured out of sight.	<input type="checkbox"/>