ENDON HIGH SCHOOL

Network Security Policy 2017-2019

Reviewed May 2017 to be reviewed every 2 years - next review May 2019

Contents

Foreword

Governing Bodies of schools are required under Financial Regulations to formally approve and implement an ICT Security Policy that complies with the County Council's minimum standards on computer security.

In order to assist Schools in this respect, Staffordshire County Council offer a drafted model "ICT Security for Schools" policy, reviewed by LMSCC and may be adopted by schools in its existing format. Endon High School has opted to use the model Policy and adapt it to their own personalised requirements.

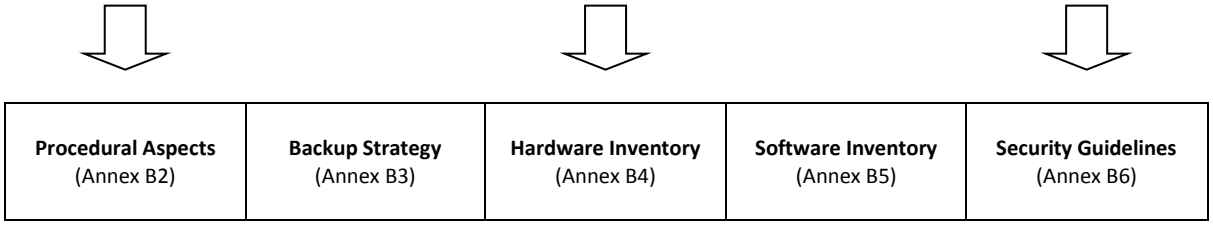
This 'model' policy represents the County Council's minimum standards on ICT security. Schools may vary this 'model' policy or draft their own ICT Security Policy, but any policy that is adopted needs to adhere to the minimum standards reflected in the 'model' policy.

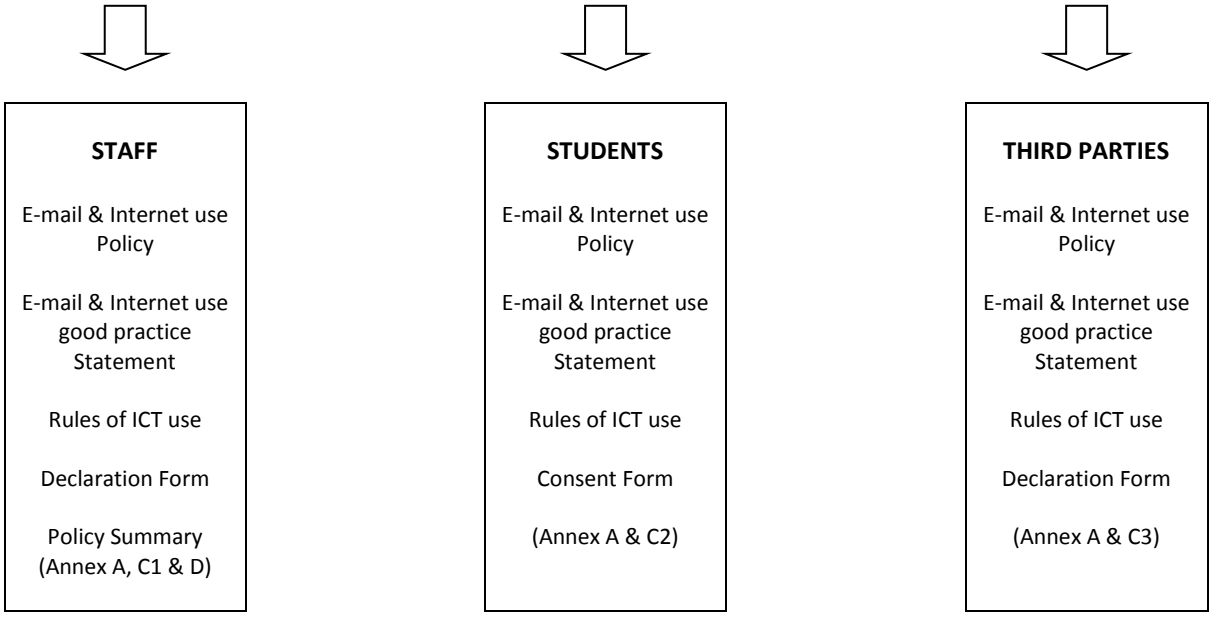
It should be noted that corporate and individual responsibilities are clearly defined within this policy. The policy requires the Headteacher to formally nominate a member(s) of school/County Council staff to carry out these responsibilities. There are also certain procedural and functional aspects of the 'model' policy that Schools must action in order to implement the policy, these are presented in Annex B2 of the policy for ease of reference. One of the key procedural aspects is the distribution of rules and agreements for ICT users, which outlines their responsibilities under the ICT Security Policy. To assist Schools in this respect, acceptable 'Rules for ICT Users' have been produced and are presented as Annex C1-C3. A summary of the key objectives of the policy is attached as Annex D. To further assist Schools in implementing the policy, a suggested strategy on the "back up" of data is attached as Annex B3 and information regarding hardware and software inventories are attached as Annexes B4 and B5 respectively. Annex B6 contains details of security guidelines to assist the System Manager in their role.

The 'model' also includes an "E-Mail & Internet Use" policy (Annex A). This refers to the "E-mail & Internet Use Good Practice Rules" for Staff and Pupils, (Annexes C1-C3) which Schools need to approve as an integral part of their ICT Security Policy. All users must complete the relevant consent or declaration form if they want to use the facilities. Endon High School implements this procedure for all newly starting Staff and Pupils (including third party users), it is then renewed on an annual basis.

ICT Security Policy for Endon High School

Implementation Programme (Annex B1)





Annex A1: Index

Information and Communication Technology (ICT) Security Policy

1. Introduction

1.1. We are managing a significant investment in the use of ICT. In many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for our needs.

1.2. Sufficient resources should be allocated each year to ensure the security of the school's 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.

2. Policy Objectives

2.1. Against this background, there are three main objectives of the ICT security Policy, these are:

a) To ensure that equipment, data and staff are adequately protected on a cost-effective basis against any action that could adversely affect the school.

b) To ensure that users are aware of and fully comply with all relevant legislation.

c) To create and maintain within the school a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

2.2. If difficulties arise in the interpretation and/or appreciation of any aspects of the policy, the Staffordshire ICT Service Desk should be consulted.

3. Application

3.1. The ICT Security Policy is intended for all School staff who have control over or who use or support the school's administration and curriculum ICT systems or data. Pupils using the school's ICT systems or data are covered by the relevant 'Rules for ICT Users' and 'E-mail & Internet Use Good Practice' documents, which are incorporated within this policy.

3.2. For the purposes of this document the terms `ICT' (or `ICT system'), `ICT data' and 'ICT user' are defined as follows:

- `ICT' (or `ICT system') means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer (whether hand-held laptop, portable, stand-alone, network or attached to a mainframe computer), workstation, word-processing system, desktop publishing system, office automation system, messaging system or any other similar device.
- `ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound.
- 'ICT user' applies to any County Council employee, pupil or other authorised person who uses the school's ICT systems and/or data.

4. Scheme of Delegation under the ICT Security Policy

4.1. The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, owner, corporate and individual levels of responsibility for ICT security are clearly defined below.

4.2. Owner

4.2.1. The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the School are the legal property of the County Council, which will normally hold it for the benefit of the School. Exceptions to this will be allowed for software and documentation produced by individual Teachers for lesson purposes, this includes scheme of work, lesson plans, worksheets or as otherwise agreed in writing by the Headteacher.

4.2.2. We also use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

4.3. Governing Body

4.3.1. The governing body has ultimate corporate responsibility for ensuring that the School complies with the legislative requirements relating to the use of ICT systems 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.

4.4. Headteacher

4.4.1. The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the School's 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 ICT security measures relating to the School's ICT facilities are applied and documented as an integral part of the policy. In practice, the day to day functions should be delegated to the 'System Manager', who must be nominated in writing by the Headteacher.

4.4.2. The Headteacher is also responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the :

- Registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data.
- Registrations are observed with the School.

4.4.3. 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. This is particularly important with the increased use of computers, laptops and tablets at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 1998.

4.5. System Manager

4.5.1. The 'System Manager' is responsible for the School's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection. The System Manager will be an employee of the School or the County Council. In many schools the Headteacher will take on the role of the System Manager. It is acceptable for technical functions to be 'out-sourced' for example to the Council's ICT Unit or use of a shared technician. Where the System Manager is not the Headteacher, the governors should be advised of the sensitivity of the post during the appointment process. In the case of Endon High School, we have a dedicated Network Manager employed by the School as well as an assistant ICT Technician.

4.5.2. Consequently, the System Manager will administer the practical aspects of ICT protection and ensure that various functions 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.

4.5.3. In line with these responsibilities, the System Manager will be the official point of contact for ICT security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of ICT security occurring within the School. The Headteacher or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

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

4.6. Internal Audit

4.6.1. The County Council's Internal Audit Section is responsible for checking periodically that the measures prescribed in each School's approved ICT Security Policy are complied with, and for investigating any suspected or actual breaches of ICT security.

4.6.2. Specialist advice and information on ICT security may be obtained from the Entrust ICT Unit, who will liaise with Internal Audit on such matters.

4.7. Users

4.7.1. All users of the School's ICT systems and data must comply with the requirements of this ICT Security Policy, the relevant rules of which are summarised in `The Rules for ICT Users' attached in Annexes C1-C3.

4.7.2. Users are responsible for notifying the System Manager 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 Internal Audit.

5. The Legislation

5.1. Background*

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

- Data Protection Acts 1984 & 1998.
- Computer Misuse Act 1990.
- Copyright, Designs and Patents Act 1988.
- The Telecommunications Act 1984 & 2000.

* You can view these legislations on the ICO website: http://www.ico.gov.uk/

5.1.2. 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.

5.1.3. The general requirements arising from these acts are described below.

5.2. Data Protections Acts 1984 & 1998

5.2.1. The Data Protection Act exists to regulate the use of computerised information about living individuals. To be able to meet the requirements of the Act, the Headteacher is required to compile a census of data giving details and usage of all relevant personal data, held on computers within the School and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 1998 Act is consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerised information.

5.2.2. 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.

5.2.3. Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

5.3. Computer Misuse Act 1990

5.3.1. 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

5.3.2. All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

5.4. Copyright Designs and Patents Act 1988

5.4.1. 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.

5.4.2. 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 licence.

5.4.3. 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 licence or contract.

5.4.4. The System Manager is responsible for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licences accord with installations. To ensure that we comply with the Copyright, Designs and Patents Act 1988 and in order to satisfy the County Council's responsibilities as a corporate member of FAST (Federation Against Software Theft), users must get prior permission in writing from the System Manager before copying any software.

5.4.5. The System Manager is responsible for compiling and maintaining an inventory of all software held by the school and for checking it at least annually to ensure that software licences accord with installations.

5.4.6. 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.

5.5. The Telecommunications Act 1984 & 2000

5.5.1. The Telecommunications Act 1984, section 43 makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'.

5.5.2. The Telecommunications Regulations 2000 impose restrictions on the interception of communications such as e-mail.

6. Management of the Policy

6.1. The Headteacher should allocate sufficient resources each year to ensure the security of the School's 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.

6.2. Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be 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.

6.3. In addition, users will be 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 ICT security.

6.4. To help achieve these aims, the relevant parts of the 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.

6.5. The Headteacher must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that 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 ICT security, and have signed the list of rules.
- A record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place.
- A record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.

7. Physical Security

7.1. Location Access

7.1.1. Adequate consideration should be given to the physical security of rooms containing 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 server rooms should be locked when left unattended. Ideally, such rooms should have a minimum of key pad access.

7.1.2. The System Manager 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.

7.2. Equipment Siting*

7.2.1. 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:

- Devices are 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 is sited to avoid environmental damage from causes such as dust and heat.
- Users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users.
- Users have been instructed not to leave hard copies of sensitive data unattended on desks.

* The same rules apply to official equipment in use at a users home.

7.3. Inventory

7.3.1. The Headteacher, 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.

8. System Security

Annex B6 contains details of security guidelines for System Managers.

8.1. Legitimate Use

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

- 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. Private Hardware & Software

8.2.1. 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 private hardware for school purposes must be approved by the System Manager.

8.3. ICT Security Facilities

8.3.1. The School's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 8. 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... For new systems, it is recommended that such facilities be confirmed at the time of installing the system. Information on the range of such facilities can be sought from Entrust ICT Unit.

8.4. Authorisation

8.4.1. Only persons authorised in writing by the System Manager, 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.

8.4.2. Access eligibility will be reviewed continually, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of the school. 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.

8.5. Access to the County Council Corporate ICT Network

8.5.1. The Headteacher must seek permission on behalf of the school for any ICT system to be linked to the County Council's corporate ICT network. In the school environment this applies to the access granted in schools to the County Council's systems for financial and creditor payments purposes. These facilities may well be extended to other areas of operation and functions of the County Council.

8.6. Passwords

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

8.6.2. Passwords for staff users should be changed at least termly and should not be re-used. They should be a minimum of eight alphanumeric characters and not obviously guessable.

8.6.3. Passwords should be memorised. If an infrequently used password is written down it should be stored securely. Passwords or screen saver protection should protect access to all ICT systems, including "boot" passwords on PCs, particularly laptop/notebook PCs as they are highly portable and less physically secure. It is acknowledged that the use of 'boot' passwords may not be feasible on Curriculum systems.

8.6.4. 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

8.6.5. Users must not reveal their password to anyone, apart from authorised staff. Users who forget their password must request the System Manager issue a new password.

8.6.6. Where a password to boot a PC or access an internal network is shared, users must take special care to ensure that it is not disclosed to any person who does not require access to the PC or network.

8.7. Backups

8.7.1. In order to ensure that our essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the System Manager, dependent upon the importance and quantity of the data concerned. A recommended strategy is presented at Annex B3.

Where programs and data are held on the Council's systems or other multi-user system, such security is likely to be covered by existing procedures. In the case of other ICT systems (including PCs) the user will normally need to make security copies of their data.

8.7.2. 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.

8.7.3. Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

8.8. Virus Protection

8.8.1. The School will use appropriate Anti-virus software for all school ICT systems. Schools are actively encouraged to conform to the recommended anti-virus protection standards. All Users should take precautions to avoid malicious software that may destroy or corrupt data.

8.8.2. The School will ensure that every ICT user is aware that any PC with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the System Manager who must take appropriate action, including removing the source of infection.

The governing body could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on School equipment.

8.8.3. Any third-party laptops not normally connected to the School network must be checked by the System Manager for viruses and Anti-Virus software before being allowed to connect to the network.

8.8.4. Teachers must take the necessary steps to ensure Anti-Virus protection software on their laptop is updated on a weekly basis as a minimum.

8.9. Disposal of Waste

8.9.1. Disposal of waste ICT media such as print-outs, floppy diskettes and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.

8.10. Disposal of Equipment

8.10.1. Prior to the transfer or disposal of any ICT equipment the System Manager 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. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations. The Data Protection Act requires that any personal data held on such a machine be destroyed.

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.

8.11. Repair of Equipment

8.11.1. 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 external media for subsequent reinstallation, if possible. The School will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

9. Security Incidents

9.1. All suspected or actual breaches of ICT security shall be reported to the System Manager or the Headteacher in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly.

The Audit Commission's Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

10. E-mail & Internet Use Policy

10.1. Attached as Annex A is the "E-mail & Internet Use Policy". This policy applies to all School staff, students and third parties who use either or both of these facilities. The conditions of use are explained in the policy. All School staff accessing these facilities must be issued with a copy of the 'Rules for ICT Users – Staff' and 'E-mail & Internet Use Good Practice' documents and complete the user declaration attached to the policy. For all students, the school will ensure that the relevant 'E-mail & Internet Use Good Practice – Rules for ICT Users - Students' document is issued and the consent form is completed by pupils and their parents. In addition copies of the 'E-mail & Internet Use Good Practice - Rules for ICT Users – Third Parties' document and consent form will be issued to all visitors. All of these documents are contained in Annexes C1–C3.

Annex A2: Part 1

Equipment Management Policy

1. Principles

1.1. The School invests very significant sums every year in the purchase of equipment to assist with pupil learning, progress and achievement, most specifically teacher laptops, interactive whiteboards, digital cameras (both stills and video) and other technology.

1.2. Laptops were provided for all teachers many years ago, in order to provide colleagues with the tools to do the job now required of them, in terms of planning and preparing interesting lessons which engage and motivate pupils, assessing progress and writing reports.

1.3. Departments and individual members of staff are entrusted with the safe and secure use of the equipment allocated to them.

1.4. As the School becomes increasingly reliant on such ICT equipment, it is necessary to be clear about where the lines of responsibility are in relation to appropriate use, and to replacement when equipment breaks down, goes missing or is damaged, etc. The County's insurance policy now requires an excess to be paid for any claim, which itself is greater than the cost of a replacement laptop. This has obviously been agreed, understandably, at Local Authority level to avoid the numerous claims which were being made for laptops.

1.5. Each new piece of equipment comes with a warranty for repair but this is nullified should the damage or malfunction be deemed to be the result of negligence on the part of the user.

1.6. Until now, the School has covered the cost of repair of expensive equipment, but there are growing concerns that this may sometimes result in a failure from staff to take responsibility for misuse or negligence. Aware that staff cannot be expected to carry out the requirements of their job now without a laptop computer, or other piece of equipment essential to a given course, there has been an expectation from staff generally that items will simply be replaced/repaired without question. Clearly this is not effective and efficient use of School resources; neither does it encourage responsibility for the property of others. Given that we are also working hard to maintain high environmental standards as part of our Eco-School work, it is part of the same rationale that we should be extending the life of expensive equipment as far as possible and not giving way to the throwaway culture which is so prevalent in today's society.

2. Aims

2.1. To support School staff in their work of raising standards of achievement by providing them with the tools to do the job required of them.

2.2. To fulfil the requirements of our School plans in terms of moving forward with modern technologies.

2.3. To ensure, as far as possible, the efficient and effective use of School resources.

2.4. To strive to extend the working life of expensive equipment through careful use and secure storage at all times.

2.5. To ensure that all staff are aware of their own and the School's respective responsibilities in relation to allocation and use of equipment, most particularly digital equipment, and its care and security.

3. Practice

3.1. All teachers* are allocated their own laptop when they take up their post at the school. This may be new or second hand, but in either case it will be installed with the appropriate programs used widely across the school. No other software should be installed without the prior consent of the ICT Systems Manager.

3.2. There is a rolling programme of laptop replacement, running over a three year cycle. The System Manager maintains a log of the type, age and reliability of each machine in school and advises the Headteacher and Bursar on which laptops should be taken out of general use and replaced each year. This is not determined in terms of personnel but in relation to the life/working order of a given piece of equipment.

3.3. All staff who have been allocated a laptop are authorised to take their laptop home without the need to sign it out formally each day. However, there is an expectation that every laptop is brought into School each working day, irrespective of the intention to use it during the day. It is school property. On no account should it be loaned to other family members.

3.4. Laptops will be taken in for general maintenance and for audit purposes on a rolling programme, sometimes at very short notice (as recommended). They will be returned as soon as possible and usually within a day or two.

3.5. Laptops must not be left in an unattended car under any circumstance. If necessary, make sure that the equipment is hidden from view – locked in the car boot for example.

3.6. Staff are asked to check their own home contents insurance policy for cover for School laptops, and explore adding this if it is not already covered. Bearing in mind that the School's insurance does not cover laptops, and that most staff use their laptops for personal as well as School use, it would seem reasonable that home contents insurance covers for accidental damage, loss or theft whilst off School premises.

3.7. When a laptop is sent off for repair, should its damage be deemed to be due to negligence and the teacher's own insurance does not cover its repair/replacement, the relevant subject area will be required to pay the cost of repair or for a replacement laptop out of departmental capitation. Whist this clearly has an impact on pupil resourcing, and the money is the School's no less than had the central budget covered the costs of repair of replacement, it is believed that this will instil a greater sense of responsibility in colleagues. The cost may be paid immediately or on a three year repayment basis.

3.8. Any other School equipment which is taken out of School must be signed out formally with the System Manager. This includes: digital cameras (both stills and video); Quizdom (key pads, receiver etc...); other relevant digital devices and other expensive equipment. The equipment should be taken home only for School purposes (for example, to prepare for a specific lesson or programme of work, to take photographs of pupils involved in an off-site activity, to train oneself in the use of the specialised equipment, etc). School equipment should not be used for home purposes unless the person concerned has discussed and agreed this with the Headteacher, who may wish to liaise with the Chair of Governors.

3.9. As with laptops, any other expensive equipment which is lost or stored negligently, resulting in theft, will be billed to the department in whose responsibility it was at the time. Similarly, should damage occur as a result of negligence, the relevant department will be billed. This is not to pass off the costs of all repairs from the central budget but to emphasise that the greatest care must be given to how, when and with whom certain pieces of equipment are used (for example, it would be considered negligent to allow certain pupils to use digital stills or video cameras whether supervised or not). The System Manager will liaise with the County Council on what constitutes negligence and what constitutes reasonable wear and tear in every case. Obviously the age and state of any item will be salient in determining future action.

3.10. When members of staff are on long-term sick or maternity leave, it is quite reasonable that their laptop should be kept in School for their replacement teacher to use. This will be agreed on an individual basis. Since there is no expectation that School work will be carried out during such long-term leave, there should be no expectation that this piece of equipment remains in the care and use of the colleague concerned.

* Should a teacher's laptop need to be repaired in the event of damage, software malfunction, warranty parts replacement job etc... The System Manager may loan a "spare" laptop (this is usually an old teacher's laptop taken out of cycle), so that the teacher in question may continue to carry out their teaching duties as normal, take class registers, write reports etc...

Annex A2: Part 2

E-mail & Internet Use Policy

1. Introduction

1.1. Schools are using E-mail and the Internet more and more to support their activities. This E-mail & Internet use policy, which will form part of our ICT Security Policy, contains the rules for using the E-mail & Internet facilities. It applies to all School staff who use either or both of these facilities.

1.2. As well as saying what you are not allowed to use E-mail and the Internet for, the policy also provides guidance on the good practices that you should use and the practices that you should avoid.

1.3. The School will periodically review the policy in response to guidance issued by the County Council.

2. Access to E-mail and Internet Services

2.1. Your connection to E-mail or the Internet must be authorised (in writing or in electronic form) by your System Manager. All School Internet access will be via an approved Internet Service Provider (ISP). Any variations to this must be authorised in writing by the Headteacher.

2.2. You must choose the ISP's filtering option if one is available.

2.3. The school E-mail and Internet facilities are for business use but we will allow staff to use them privately, as long as it is reasonable. If you use these facilities, you must keep to, and not break any of the conditions in this policy.

2.4. The School has the right to monitor E-mails and Internet use.

2.5. If you intentionally access a computer system or information without permission, you are breaking the law under the Computer Misuse Act 1990.

3. Code of Conduct Declaration

3.1. If you use or have access to our E-mail or Internet facilities, you need to read this policy carefully and make sure that you understand it. The school will provide appropriate training. You then need to sign the declaration/consent form (see Annex C1-C3) to confirm that you have read, understood and will keep to the policy. You must also understand that we may take action against you if you wilfully break the conditions of the policy.

3.2. The School will keep the signed declaration in your personal file. Sometimes, we may ask you to confirm that you still understand and accept the rules.

3.3. Students and employees logged into a computer shall be considered to be the person browsing the Internet (this also includes third party users). Under no circumstances shall any student or employee browse the Internet from an account belonging to another person.

3.4. The School shall monitor and log all Internet access by students, employees and third party users and reserve the right to disclose this information to any relevant authority.

4. Specific Conditions of Use

4.1. General Prohibitions

4.1.1. You must not use, or try to use, our E-mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies. In this context, you are not allowed to use the E-mail and Internet facilities for reasons that are:

- Pornographic or obscene.
- Intimidating, hateful and discriminatory (for example; racist, sexist, homophobic, age, religious beliefs etc...) or that break our anti-harassment and equal opportunities policies in any other way.
- Defamatory, slander and libel.
- Encouraging violence, criminal acts or strong feelings.
- Fraudulent.
- Unethical or may give the School bad name.
- A deliberate harmful attack on systems we use, own or run.
- Sexually explicit messages, images, cartoons, jokes, audio or movie files.

4.1.2. We will only allow you to do the above if:

- It is part of your job to investigate illegal or unethical activities.
- Your Headteacher or System Manager asks you to in writing.
- It is in the public interest.

You must make sure that your System Manager knows what you are doing. If you find or suspect anyone of using the computer system illegally or unethically, you must report it to your System Manager who will advise your Headteacher or Chair of Governors or Internal Audit.

4.1.3. You must not use the school E-mail or Internet facilities for time-wasting activities, such as chain letters, or for sending private E-mails to everyone on the global address list.

4.2. Computer Viruses

4.2.1. It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. You must not use the school E-mail and Internet facilities for:

- Intentionally accessing or transmitting computer viruses or other damaging software.
- Intentionally accessing or transmitting information about, or software designed for, creating computer viruses.

4.2.2. You must scan any material you receive or download from the Internet to make sure it is virus free. The school will ensure that virus protection exists on any standalone or locally networked computers that can access the Internet and train you in its use. You must not E-mail material that has not been scanned to other users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and tell your System Manager.

4.2.3. You must always follow the instructions that your System Manager gives you about virus attacks.

4.2.4. If you are not sure how to use the virus protection system, you must get advice from your System Manager.

4.3. Passwords

4.3.1. You must not tell anyone your password, apart from authorised staff.

4.4. Other Security

4.4.1. You must not use or try to use the school facilities for:

- accessing or transmitting information about, or software designed for, breaking through security controls on any system;
- breaking through security controls on any system; or
- accessing, without permission, any E-mail that is not for you, even if it is not protected by security controls.

4.5. Publishing Information

4.5.1. You must get authorisation from the Headteacher for any school information that is to be published on the Internet. All schools have web space available for authoring of their own school web site. Images of individuals must have their permission or that of their parent/guardian before publication of the web site (see Annex C2). We will not allow the publishing or editing of Web sites which involve advertising, financial reward or are part of a business.

4.6. Copyright

4.6.1. It is illegal to break copyright protection. You could break copyright if you download or transmit protected material through E-mail or over the Internet.

4.6.2. You must not

- transmit copyright software from your computer to the Internet or allow any other person to access it on their computer through the Internet; or
- knowingly download or transmit any protected information that was written by another person or organisation without getting permission from the owner.

Permission can be sought via E-mail.

4.7. Confidential or Sensitive Information

4.7.1. You must not break the conditions of the Data Protection Act 1998 when you use the E-mail services of the Internet for transmitting information.
If you need any more advice about these conditions, you should refer to the Policy summary or obtain further information/advice from the System Manager.

4.7.2. The Internet E-mail facility is not a secure way of transmitting confidential, sensitive or legally privileged information unless there are special security measures (such as encryption). Without these security measures, Internet E-mail is as insecure as a postcard that you send through the normal post. So, you should make sure that the Internet is suitable for transmitting information that you feel is confidential, sensitive or legally privileged. If you allow anyone to see this type of information without permission, you may be breaking the law.

4.7.3. If you have to transmit any E-mail over the Internet that you think contains confidential, sensitive or legally privileged information, no matter what special security measures you take, you are strongly advised to include the following disclaimer in the E-mail.

'This E-mail (including any attachments) is only for the person it is addressed to. If you are not this person, you must delete this E-mail immediately. If you allow anyone to see, copy or distribute the E-mail, or if you do, or don't do something because you have read the E-mail, you may be breaking the law'. This disclaimer can be set using the 'autosignature' facility where this is available.

4.8. Bulletin Board

4.8.1. There are 'bulletin boards' (electronic notice boards) on the County Council's Intranet and the SLN Internet site for discussion, social and personal use. These 'bulletin boards' are moderated to ensure appropriate use. The conditions of use in this policy also apply to the bulletin boards.

4.8.2. Neither the school, the LEA nor the County Council is responsible for the content of any material included in the bulletin board or for anything users do because of the material.

5. Recording Internet Use

5.1. You should be aware that use of ISP facilities is logged.

5.2. If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to your System Manager or Headteacher. If you do not do this, the school may take action against you.

5.3. You should protect yourself by not allowing unauthorised people to use your Internet facility.

6. E-mail Good Practice

6.1. Annex C1–C3 contains guidelines that tell you what is and what is not good practice when you use internal or Internet E-mail services.

Annex B1: ICT Security Policy

Implementation Programme

Each of these documents will need to be reviewed on a regular basis. Completing the following table will document the policies adopted by the school and assist in identifying the relevant review process. Any other implementation issues can also be documented in the following section.

Documents relating to ICT Security for Schools

Document Name	Model Document used?	Location of Document	Produced and/or Reviewed by...	Last Review Date	Next Review Date
ICT Security Policy					
E-mail & Internet Use Policy (Annex A)					
Procedural Aspects (Annex B2)					
Backup Strategy (Annex B3)					
Hardware Inventory (Annex B4)					
Software Inventory (Annex B5)					
Security Guidelines (Annex B6)					
Rules for ICT Users – Staff (Annex C1)					
E-mail & Internet Use Good Practice for Staff (Annex C1)					
Declaration form for Staff (Annex C1)					
E-mail & Internet Use Good Practice - Students (Annex C2)					
Pupil/Parent Consent Form (Annex C2)					
E-mail & Internet Use Good Practice - 3rd parties (Annex C3)					
Consent form for 3rd Parties (Annex C3)					

Nominated System Manager:	
Other Implementation Issues:	

Annex B2: ICT Security Policy

Procedural Aspects of the Policy

	Notes
1.	The Governing Body must ensure that the School implements an ICT Security Policy - this can either be the 'model' policy or the School can create an amended policy based upon the 'model'. This must be reviewed annually and must include Email and Internet Use Policies for staff and pupils.
2.	The Headteacher must nominate a System Manager or members of non-teaching staff with designated systems management responsibilities. It must be documented (in Annex B1 of the model policy) and included in the Scheme of Delegation approved by the Governing Body. The Headteacher must ensure that the nominated member(s) of non-teaching staff understands the functions of the role and is familiar with the relevant Acts.
3.	The Headteacher must compile a census of data giving details and usage of all personal data held on computer and manually (as required under the Data Protection Act 1998) in the School, and file a registration with the Data Protection Registrar. Users should be periodically reminded of the requirements of the Data Protection Act, particularly the limitations on the storage and disclosure of information.
4.	The Headteacher should ensure that a copy of the relevant 'Rules for ICT Users' (attached as Annex C1-C3) is issued to all system users. This should include all relevant aspects of the ICT Security Policy and any other information on the use of facilities and techniques to protect the systems or data. This will include: • Inappropriate use of E-mail and the Internet. • Breaches of security - reporting procedures. • Use of private hardware and software. • User authorisation process. • Access rights. • Equipment siting, room layout, physical security. • Appropriate use of the School facilities.
5.	The Headteacher should retain a record of: • The distribution of the 'Rules for ICT Users' - to staff, students and third parties; • The access rights to systems and data granted to individual users; • Any amendments or withdrawal of these rights due to a change in responsibilities or termination of employment or starters/leavers; • The training provided to each individual user.

6.	An inventory of all ICT equipment must be maintained and regularly updated by the System Manager as equipment is purchased/disposed of. The inventory must be checked and verified annually in accordance with the requirements of Financial Regulations. (Recommended Pro-forma attached as Annex B4).
7.	The Headteacher should define local rules regarding the use of privately acquired hardware and software, which should be disseminated to all computer users. This will also include use of non-approved E-mail accounts.
8.	An inventory of all software and licence details must be maintained and regularly updated by the Systems Manager as software is purchased/disposed of. The inventory must be checked annually to ensure that the licences accord with installations. (Recommended pro-forma attached as Annex B5). The System Manager should ensure that there are clear procedures regarding the installing/copying of software. The System Manager should be familiar with the requirements of FAST (Federation Against Software Theft).
9.	The System Manager should ensure that there are clear procedures regarding installing, upgrading, repairing and the disposal of equipment.
10.	The System Manager must decide on the appropriate frequency for password changes and give advice on the technique for password selection based on the value and sensitivity of the data involved, and give advice to users accordingly. The System Manager must ensure there are clear procedures regarding the disposal of equipment and waste containing confidential or sensitive data.
11.	The System Manager must ensure that a backup strategy is agreed, documented and implemented. Clear instructions must be given to users to ensure this is followed (recommended strategy attached as Annex B3).
12.	The System Manager should confirm and implement a policy on Anti-Virus software for local networks, standalone systems, laptops and home PCs (particularly where data may be transferred to School). This must ensure that anti-virus software is regularly updated.
13.	The System Manager must distribute the "E-mail & Internet Use Policy for Schools" (Annex A) to all users and ensure that they complete the relevant user declaration attached to the policy.

Annex B3: ICT Security Policy

Backup Strategy for Endon High School

- All data is incrementally backed up on a daily basis, a full backup is taken at the end of every week. Backups are taken from the servers.
- Backups are stored in a fire proof safe in the library, the library is located in a separate building off from the main School.
- All backups are checked to ensure that they have been successful, we check the contents of the backup drive to make sure that data has been written, and that the data is dated consistent with the backup date.
- LRM/FMS users are strongly recommended to backup the financial files before any reconciling (manual or automatic) is undertaken. Label the disk with the month during which the backup was taken, and keep it for at least 12 months for future restore purposes, if ever required.
- A 'Long-Term Backup' is taken at the end of each term. It is kept and not overwritten until the beginning of the next term. This will help to protect against data corruption that goes unnoticed for several weeks, during which 'older' backups will have been overwritten by 'newer' ones.
- If any problems should arise with our current backup media, we have an external hard drive in place which will be used to backup data on a temporary basis, until Entrust can assist us in getting our system back up and running.
- If possible, personal backups of data must be created. Either on the School network or removable media. If using removable media (such as USB drives), you must ensure that any sensitive data is encrypted.
- If we ever have queries about backups, we telephone the Entrust ICT Service Desk and check whether or not the current processes are adequate and reliable.

Annex B4: ICT Security Policy

Hardware Inventory

We log every hardware item in School. When new equipment arrives we PAT test it and add it to the Assets Register.

Annex B5: ICT Security Policy

Software Inventory

We log every software program in School. When new software arrives we add it to the Software Register.

Annex B6: ICT Security Policy

Security Guidelines

1. Password Policy

1.1. Passwords should be:

- Unique.
- Alphanumeric.
- At least 8 characters in length.
- Regularly changed, at least every 90 days.

1.2. Passwords should not be:

- Written down.
- Easy to guess, for example, a single word such as “password”.
- Shared with any other people, including family and friends.

2. Monitoring Computer Use by Pupils

- Ensure pupil use of computers is 'visual', make sure there is a responsible person present and monitoring use.
- Consider logging access to the network using software tools, for example Tutor.
- Review the layout of the room to ensure there is good 'visibility' of computer activities.
- Ensure there is supervision at all times.
- Publish the ‘Rules of ICT Use’ next to the computers, or consider displaying them on the screen when the computer is turned on. Please see AUPs attached to this policy.
- Maintain an audit trail of user activity.

3. Monitoring Computer Use by Staff (especially in sensitive areas)

- Use screensavers with passwords.
- Consider using 'distinctive' background colours.
- Think carefully about the siting/location of equipment.
- Take care when disposing of paper output, storage media, computers etc... that may contain sensitive or personal information.

4. System Backup

- Make sure the system is backed up and periodically tested.
- Try to implement an automated system backup.
- Make sure the instructions for re-installing data or files from a backup are fully documented and readily available.
- Use 'off-site' storage for backup where possible.
- Consider using different media as a secondary backup facility.

5. Anti-Virus Protection

- Always use an approved and recommended product, we use Symantec Endpoint Protection v12 at Endon High School.
- Make sure there is a process to ensure it is regularly updated and all equipment is included, this is especially important for stand-alone PCs, laptops and computers used at home.
- Make sure there is a clear procedure for dealing with any actual or suspected infections – this usually involves isolating the system from the network and removing the infection in a stand-alone condition.
- Make sure the process for 'cleaning' infections is documented – this may involve requesting assistance from SLT.

6. Illegal or Inappropriate Use of the Network

- Make sure there are appropriate procedures in place for auditing access to the network and systems.
- Regularly check the network for 'unauthorised' files.
- If possible, ensure auditing is performed both at the Management System level and also at the Operating System level.
- Software to assist with auditing - this can help monitor activities such as logons, file usage etc...
- Consider using a firewall or proxy server to restrict external activity and access. We use Entrust Broadband Solution for our proxy server.

7. Internet Use/Filtering

- Make sure an Internet Use policy has been adopted for each 'category' of User and all Users have signed up to it.
- Define and document any local agreements/policies on restricting websites, access to newsgroups and chat-rooms etc...
- Obtain parental permission where appropriate.
- Ensure there is a clear process for reporting any access to inappropriate material.
- Consider restricting specific functions such as the downloading of EXE, MP3 files etc...
- Publish safe guidelines.
- Make sure Internet use is supervised.

8. E-mail Use

- Make sure an Email Use policy has been adopted for each 'category' of User and all Users have signed up to it.
- Define and document any local policy on the use of E-mail and E-mail addresses, including the use of 'non-approved' E-mail accounts.
- Consider implementing limits on inbox sizes, size and types of attachments etc...
- Be clear about what is considered 'appropriate' use of E-mail and language.
- Involve staff, parents and students in these decisions.

9. Documentation

Ensure adequate documentation is available for:

- The network infrastructure.
- The network systems, hardware, software etc...
- Administration procedures.
- ICT Security Policy for Endon High School.
- Housekeeping procedures.
- Problem resolution.
- Ensure support disks, recovery disks, backups etc... are available.

10. Training

- Ensure there is adequate training for the System Manager and computer users.
- Introduce 'good practice' guidelines where appropriate, for example; using screensavers with passwords.

11. Authentification/Operating System Level Security

- Consider using system policies to provide additional security.
- Ensure there is a rigorous policy for approval/removal of users.
- Avoid the use of 'generic' accounts, where their use is unavoidable set up only for the duration of the particular requirement.
- Limit the number of Administrator and Manager accounts.
- Avoid the use of Groups with Administrator or Manager rights.
- Only log on as Administrator or Manager when performing functions requiring this level of access, use an ordinary level User account where this is not required.
- Set clear security levels on the network and ensure these are documented and followed.
- Restrict access to applications and data areas where appropriate.
- Consider using 'read only' access where possible.

12. Network Review

- Monitor system downtime, ensure there are support arrangements in place to react to problems with critical equipment or infrastructure.
- Monitor performance of the network – ensure there is a process in place to develop and upgrade the network infrastructure and equipment as necessary.
- Monitor service disruption – ensure support arrangements are in place to resolve problems in a timely fashion.
- Regularly review appropriate documents e.g. Computer Security policy, E-mail & Internet Use policies, this could include reviewing official documents such as the BECTA 'Superhighway Safety'.
- Review procedures for dealing with all security breaches or compromises, whether deliberate or innocent.

13. Monitor System Usage

- You should make all users aware that that the systems they are using are the property of the School and that there can be no expectation of privacy.
- You should make users aware that the School manage the E-mail system which means that the school also own all copies of messages created, received or stored in the Microsoft 365 cloud. The users should be made aware that no E-mails will be private, even if marked as “private” and/or “confidential” or with any similar wording.
- All E-mails are stored in the Microsoft 365 cloud we do not allow client programs such as Outlook to store and transfer E-mails on a laptop or pc.

14. Protective Marking

- It is important to provide adequate protection to information, an additional tool which can assist in this is a protective marking scheme. All documents should be protectively marked, either using the government scheme that is recommended by BECTA, or by an internal classification scheme.
- A protective marking scheme is a way of assigning information to a security level which, in turn, relates to a range of pre-defined controls designed to ensure the information is handled properly.
- From 6th April 2010 the Information Commissioner will have new powers to fine organisations up to a maximum of £500,000 for data security breaches. A protective marking scheme is one of the activities you can undertake to ensure the security of the information that you hold.

15. Hardware & Software Inventory

- In order to comply with the School’s Financial Regulations, you must maintain an inventory of all ICT equipment (however financed) which must be audited at least annually.
- The use of all private hardware for school purposes must be approved by the System Manager.
- A comprehensive inventory of all software and licence details should be maintained and regularly updated as software is acquired or disposed of. If software is used illegally because it is not licensed it could result in a fine or in extreme cases a jail sentence.

16. Transferring Data

- Any data that is to be transferred outside of the School must be encrypted.
- Data held on USB storage devices, laptops or other removable media such as CDs must be encrypted to a minimum standard of 256 AES.
- Sensitive data that is being transferred by email must be encrypted.

Annex C1: ICT Security Policy

Rules and Agreements for Staff (Rules for ICT Users – Staff)

	Notes
1.	Ensure you know who is in charge of the ICT system you use, i.e. the System Manager.
2.	You must be aware that any infringement of the current legislation relating to the use of ICT systems : • Data Protection Acts 1984 & 1998 • Computer Misuse Act 1990 • Copyright, Designs and Patents Act 1988 • The Telecommunications Act 1984 Provisions of this legislation may result in disciplinary, civil and/or criminal action.
3.	ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of data held.
4.	Follow the local rules determined by the Headteacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be copied if specifically approved by the System Manager.
5.	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat. Do not leave you computer logged on, i.e. where data can be directly accessed without password control, when not in attendance. These same rules apply to official equipment used at home.
6.	You must not exceed any access rights to systems or limitations on the use of data granted to you by the System Manager.

7.	The System Manager will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use. You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a "made up" word, but not obvious or guessable, e.g. surname; date of birth. Do not divulge your password to any person, or use another person's password, unless specifically authorised to do so by the System Manager, e.g. in cases of shared access. Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle/drawer to which only you have access.
8.	The System Manager will advise you on what "back ups" you need to make of the data and programs you use and the regularity and security of those backups.
9.	Ensure that newly received floppy disks, CD ROMs and emails have been checked for computer viruses. Any suspected or actual computer virus infection must be reported immediately to the System Manager.
10.	Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, floppy disks, etc.
11.	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Headteacher, Chair of Governors or Internal Audit.
12.	Users of these facilities must complete the declaration attached to the "E-mail & Internet Acceptable Use Policy".

Annex C1: ICT Security Policy

Rules and Agreements for Staff (E-mail & Internet Use Good Practice)

The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or Internet E-mail services:

1. **You should:**

- Check your E-mail inbox for new messages regularly;
- Treat E-mail as you would a letter, remember they can be forwarded/copied to others;
- Check the message and think how the person may react to it before you send it;
- Make sure you use correct and up-to-date E-mail addresses;
- File mail when you have dealt with it and delete any items that you do not need to keep.

2. **You should not:**

- Use E-mail to manage Staff where face-to-face discussion is more appropriate;
- Create wide-distribution E-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- Print out messages you receive unless you need a hard copy;
- Send large file attachments to E-mails to many addressees;
- Send an E-mail that the person who receives it may think is a waste of resources;
- Use jargon, abbreviations or symbols if the person who receives the E-mail may not understand them.
- Upload any photographs of pupils or use any for display purposes until you have checked that parents or guardians have given appropriate permission – using the consent form in Annex C2

Annex C1: ICT Security Policy

Rules and Agreements for Staff (Staff Declaration)

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in your personal file.

Declaration

I confirm that, as an authorised user of the School's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Rules for ICT users - Staff, and the conditions in the E-mail and Internet use policy, including those in the 'E-mail & Internet Use Good Practice'.

Your details

Name: _____

Job title: _____

Signature: _____ Date: _____/_____/_____

Annex C2: ICT Security Policy

Rules and Agreements for Students (E-mail & Internet Use Good Practice)

The school computer system provides Internet access to students for learning. This E-mail and Internet Use Good Practice statement will help protect students and the school by clearly stating what is acceptable and what is not.

- School computer and Internet use must be appropriate to the student's education.
- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Storage media (USB drives, CDs, Floppy Disks etc...) must not be brought into school unless permission has been given.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others which might be stored in common shared areas on the system. Conversely, users should always try and store their files and data in their own secure area. Files and data stored in common shared areas of the system must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms or instant messaging is not allowed.
- The school ICT systems may not be used for private business purposes, unless the Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whoever they belong to.
- Irresponsible use may result in the loss of Internet access or even an account suspension.

Endon High School may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Annex C2: ICT Security Policy

Rules and Agreements for Students (Consent Form)*

Endon High School

Responsible E-mail & Internet Use

Please complete, sign and return to the School secretary

Pupil Name:	Form:
Pupil Agreement I have read and understand the school 'E-mail and Internet Use Good Practice - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	Date:

Parent/Carer Name:
<u>Please tick each box that you agree to:</u> ❑ **Parent/Carer Consent for E-mail & Internet Access** I have read and understood the school 'E-mail and Internet Use Good Practice - Rules for ICT Users' document and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. ❑ **Parent/Carer Consent for Web Publication of Work and Photographs** I agree that, if selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used. *Staff must check the consent forms before they use any pictures of students.*
Signed: Date:

* Based on the Internet Policy of the Irish National Centre for Technology in Education.

Annex C2: ICT Security Policy

Rules and Agreements for Students (Sample Letter to Parents)

Endon High School
Leek Road
Endon
ST9 9EE
01782 502240

1st January 2012

Dear Parent/Carer,

As part of your child's curriculum and the development of ICT skills, Endon High School is providing supervised access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached 'E-mail and Internet Use Good Practice - 'Rules for ICT Use' document, and sign and return the consent form so that your child may use Internet at school.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please contact me to arrange an appointment.

Yours sincerely,

Mrs. A. Gibson
Headteacher

Annex C3: ICT Security Policy

Rules and Agreements for Third Party Users (E-mail & Internet Use Good Practice)

The school computer system provides Internet access to students for learning. This E-mail and Internet Use Good Practice statement will help protect students and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Storage media must not be brought into school unless permission has been given.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others which might be stored in common shared areas on the system. Conversely, users should always try and store their files and data in their own secure area. Files and data stored in common shared areas of the system must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms or instant messaging is not allowed.
- The school ICT systems may not be used for private business purposes, unless the Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whoever they belong to.
- Irresponsible use may result in the loss of Internet access or even an account suspension.

Endon High School may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Annex C3: ICT Security Policy

Rules and Agreements for Third Party Users (Consent Form)*

Endon High School

Responsible E-mail & Internet Use

Please complete, sign and return to the School secretary

IMPORTANT INFORMATION FOR THIRD PARTY USERS:

Please make sure that you read and fully understand our Acceptable Use Policy **before** logging onto the School network, School E-mail system and our Virtual Learning Environment.

Full Name:	Company:
	Address:
Third Party User Agreement I have read and understand the school 'E-mail and Internet Use Good Practice - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	Date:

* Based on the Internet Policy of the Irish National Centre for Technology in Education.

Annex C4: Acceptable Use Policy

Firefly

All users of Firefly are required to sign up to this acceptable use policy when they log on for the first time. They must accept the conditions set out below in order to access any material. Please note these conditions apply to the whole duration of you using Firefly.

If you breach any of these conditions, the School may regard this as misconduct. In appropriate cases the School will deal with such breaches under the Behaviour Management policy. Misconduct on Firefly, whether it occurs during School time or not, shall be dealt with equally.

Security
Each individual is responsible for the security and use of their username and password. You are not allowed to use the account, username or password of any other user. You must not disclose your username or password to anyone else.

Communication
When using Firefly's communication facilities you must:

- Respect other people's views and beliefs.
- Only post comments which are appropriate to the particular discussion.
- Remember that you are conversing with real people and not with a screen name in cyberspace.

This will enable you to enjoy your interaction with fellow Firefly users in a friendly and intellectually stimulating environment.

By contributing postings to any forum within Firefly you are granting a license to the School to reproduce the content of your posting, and you are also granting a license to other users to download or copy the content in accordance with these conditions.

When using Firefly 's communication facilities you must not:

- Post anything abusive, defamatory, obscene or otherwise illegal.
- Post any personal or private information on any individual.
- Copy or forward E-mail or any other private messages without permission.
- Include material which is confidential or the copyright of which is owned by someone else, unless you have first obtained permission.
- Post material which contains viruses or other programs which may disrupt the School's systems.
- Post any advertising or promotional material.
- Behave in an impolite or offensive manner.

Endon High School reserves the right to remove, vary or amend any of the content which appears on Firefly at any time and without prior notice.

When submitting postings or assignments within Firefly you must give due acknowledgement for material quoted from other sources, both within Firefly and elsewhere.

Copyright

Copyright of the study material and all other content of Firefly are owned or controlled by Endon High School.

You are permitted to view, copy, and print documents within Firefly subject to your agreement that:

- Your use of the material is for your own personal information and for non-commercial purposes only.
- You will not modify the documents or graphics in any form or manner.
- You will not copy or distribute graphics separately from their accompanying text and you will not quote materials out of their context.

Annex C4: Acceptable Use Policy

Network (Curriculum & Admin): Updated – April 2008

You must accept these rules when you log onto the School network.

Internet & E-mail

You must:

- Only access websites that are relevant to your school work.
- Respect copyright and trademarks, give credit to anyone who's work you use.
- Check with a member of staff before completing online questionnaires.
- Do not fill out subscription forms unless otherwise stated by a member of staff.
- Ensure that all E-mail messages that you send are not offensive.
- Regularly delete unwanted E-mail messages.

You must not:

- Play or download games from the Internet.
- Download applications from the Internet in any file format.
- Use online chat or web-based email messaging such as Hotmail or Yahoo.
- View offensive content such as pornography, violence or racial material.
- Use online community websites such as Facebook or Twitter.
- Cyber bully, we have zero tolerance for any such behaviour.
- Use any type of proxy to bypass the network filtering systems.
- Send, access or display offensive messages.
- Send any personal information to anyone, even if you know them.
- Use or send language of an inappropriate nature.
- Open E-mail attachments, even if they are from a reliable source.
- Send messages to group E-mail aliases such as the all student setup.

Printing

You must:

- Only print documents that are relevant to your work.

You must not:

- Print excessive copies of documents unless stated by a member of staff.
- Print entire documents where a single sentence is required.

User Area

You must:

- Only store files in your area that are relevant to your work
- Delete files that are no longer required
- Keep your user area organised and indexed correctly

You must not:

- Store offensive or prohibited content in your area, including executables
- Store songs in any type of audio format unless you have permission from staff

Passwords

You must:

- Change your password on a regular basis, preferably every half term
- Ensure that your password is between 6-10 characters long and alphanumeric
- Ensure that only you know your password
- Come straight to the technicians office if your password does not work

You must not:

- Log onto the network as anyone else but yourself
- Write your password down, please try to remember it!

Removable Storage

You must:

- Ask a member of staff before using any type of removable storage
- Safely remove your USB device to ensure no data is lost

You must not:

- Plug any type of removable media into the computers USB ports unless told to
- Use the USB ports on any of the computers to charge your USB device

What will happen if these rules are broken?

- Your user account and/or access to the Internet will be disabled.
- If you repeatedly break the rules then you could be suspended.
- Parents and senior management will be involved with serious breaches of the rules.
- The Police will be involved with any criminal related issues.

All computer use is being monitored by the computer technicians, please be aware that records are kept of all inappropriate computer usage. The technicians may monitor your computer if they see anything suspicious.

Please report all breaches in security to the ICT Department.

Annex D1: ICT Security Policy

Policy Summary

The objectives of the Policy, which is intended for all school staff, including governors , who use or support the school's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all 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.

The integrity of the Staffordshire schools' network depends on the security policy implemented by each connected school.

Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The school's System Manager is responsible for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The System Manager will be the official point of contact for ICT or information security issues.

Responsibilities:

- ✓ Users of the school's ICT systems and data must comply with the requirements of the ICT Security Policy.
- ✓ Users are responsible for notifying the System Manager of any suspected or actual breach of ICT security. In the absence of the System Manager, users should report any such breach directly to the Headteacher, Chair of Governors or to the Council's ICT Unit.
- ✓ Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- ✓ Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- ✓ Adequate procedures must be established in respect of the ICT security implications of personnel changes.

Physical Security:

- ✓ As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- ✓ Server rooms must be kept locked when unattended.
- ✓ Appropriate arrangements must be 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 and software should be recorded and an inventory maintained.

- ✓ Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
- ✓ Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- ✓ Equipment should be sited to avoid environmental damage.
- × Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- × Do not give out sensitive information unless the recipient is authorised to receive it.
- × Do not send sensitive/personal information via e-mail or post without suitable security measures being applied.
- ✓ Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security:

- × Users must not make, distribute or use unlicensed software or data.
- × Users must not make or send threatening, offensive or harassing messages.
- × Users must not create, possess or distribute obscene material.
- ✓ Users must ensure they have authorisation for private use of the school's computer facilities.
- ✓ The System Manager will determine the level of password control.
- ✓ Passwords should be memorised. If passwords must be written down they should be kept in a secure location.
- × Passwords should not be revealed to unauthorised persons.
- × Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- ✓ Passwords should be changed at least once per term.
- ✓ Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- ✓ Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- ✓ Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- ✓ Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection:

- ✓ The System Manager will ensure current and up to date anti-virus software is applied to all school ICT systems.
- ✓ Laptop users must ensure they update their virus protection at least weekly.

- ✓ The System Manager will ensure operating systems are updated with critical security patches as soon as these are available.
- ✓ The System manager will ensure users of home/school laptops check for critical security patches/Anti-virus updates when connecting laptops to the school network.
- ✓ Any suspected or actual virus infection must be reported immediately to the System Manager.

Disposal and Repair of Equipment:

- ✓ The System Manager must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
- ✓ It is important to ensure that any software remaining on a PC 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 System Manager must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.
- ✓ The school will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

Security Incidents:

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the System Manager, or Headteacher in their absence, who should report the incident to the Staffordshire ICT Service Desk (01785 278000).

This policy is to be used in conjunction with the ESafety Policy