Blue Hills Federation

ICT SECURITY POLICY

SEPTEMBER 2023

The Blue Hills Federation

The Blue Hills Federation is a collective of three primary schools – Clunbury CE Primary School, Newcastle CE Primary School and St Mary's Bucknell CE Primary School. All three schools share one Executive Headteacher and one Governing Body. When using the term 'Blue Hills Federation' within this policy, it is in reference to all three schools. When policy only applies to one school that school will be named specifically. Newcastle CE Primary School does not have a nursery or a preschool, therefore any references to nursery or pre-school do not apply to Newcastle CE Primary School.

Our Vision

Proverbs 22:6 - Good News Bible

'Teach children how they should live, and they will remember it all their lives.'

We are a caring Church Federation bringing together and serving many communities.
We provide nurturing environments that facilitates learning for all. We encourage everybody to become confident, sociable and responsible citizens who achieve to the best of their ability in preparation for a fulfilling future.

Our Values

Trust and Truth; Joy and Happiness; Love and Respect; Thankfulness; Friendship and Family; Perseverance and Resilience

Review Date: September 2024

Information and ICT Security Policy and Guidance

Status

This policy is recommended to schools and is based on good practice.

Purpose

The objectives of this Policy are to:

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

Consultation

At local authority level, comments have been sought from the following groups:

- Secondary school network managers
- ICT Advisers
- Information Governance
- Headteachers' ICT and eLearning Group
- Staff and pupils in school

Relationship with other policies

Policies are written and reviewed at different times and they should not contradict. Note other guides and policies here to enable a coherent approach.

Arrangements for monitoring and evaluation

GBs need to be reminded that it is their responsibility to monitor or review this policy and for this to be done within a framework of planned policy review via the GB's committees.

Introduction to Guidance

Schools have made a significant investment in computer systems and networks and reliable ICT services are vital to teaching, learning and management tasks. In addition, schools manage personal and sensitive information.

The majority of Shropshire schools have access to the Shropshire wide area network (WAN), providing them with access to corporate resources such as Samis and ResourceLink.

This wider access places a responsibility on all participating schools to ensure that their 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.

Definitions

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

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

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.

The Policy should be reviewed by the Governing Body/Schools on an annual basis.

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

Model acceptable use policies are also incorporated as appendices to this document. Those for learners, adults working with young people and the guidance notes for schools and governors are those originally issued by WMNet in 2009.

Responsibilities

The Governing Body

The Governing Body has ultimate responsibility for ensuring that the schools comply 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 Executive Headteacher.

The Executive Headteacher

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

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

In addition, the Executive 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 E 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 organisation's response. Typically, the SIRO should be a member of the senior leadership team in a secondary school and may be the headteacher in a primary school. The following responsibilities attach to the role of SIRO:

- They own the information risk policy and risk assessment
- They appoint the Information Asset Owners (IAOs) – see section 0
- 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 schools to each individual user will be maintained.

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

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

- The 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 may also be responsible for the schools' ICT equipment and systems 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.

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 Executive Headteacher or Chair of Governors of any suspected or actual breach of ICT or information security occurring within the schools.

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 Anna Cook

Information Asset Owner (IAO)

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

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

An information asset is regarded as the collection of data or an entire dataset. It is important to distinguish between an information asset and the information (usually a subset of the asset) that needs protection. For example, reports run from an information asset, such as SIMS, are not information assets themselves.

There should be an IAO for each asset or group of assets as appropriate. For example, the SIMS database should be identified as an asset and should have an IAO.

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 schools' Information Asset Owners are: Anna Cook, Juliet Morgan, Abby Garnett and Steph Reynolds.

Audit Services

The Audit Services section of the Council is responsible for checking periodically that the measures prescribed in each school's approved Information and ICT Security Policy are complied with.

Users

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

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

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

Legislation Background

The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems and information security. A full list of legislation can be found on the ICO (Information Commissioner's Office) website – ico.org.uk

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

Management of the Policy

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

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

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

Physical Security Location Access

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

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

All school owned ICT equipment should be recorded and security-marked. Advice on security marking is available from Shropshire Council's Crime Prevention Officer.

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

Siting of Equipment

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

- Information (paper or electronic) should be protected in such a way that it cannot be accessed or viewed by persons not authorised to access it.

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

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

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

Physical Security – Checklist

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

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.

See appendix D for a sample form to record the disposal of assets.

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 schools' equipment is acquired from a responsible source and is used strictly in accordance with the terms of the license. The use of all personal hardware and software for school purposes must be approved by the SIRO.

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

Inventory – Checklist

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

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 appendices)

Legitimate Use

The schools' ICT facilities must not be used in any way that breaks the law or breaches School policy.

Such breaches include, but are not limited to:

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

ICT Security Facilities

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

Administrative and curriculum network traffic is separated by the use of virtual LANs (Vlans) across the broadband network. Schools wishing to allow cross network traffic must ensure that there are adequate security measures in place to preserve the confidentiality, integrity and availability of sensitive data.

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

Authorisation

Only persons authorised by the SIRO, are allowed to use the schools' ICT systems. The permissions allocated to a user will be sufficient for needs but not excessive.

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

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

Access eligibility will be reviewed continually, including remote access to systems and external web services, eg Secure Access. In particular, the relevant access capability will be removed when a person leaves the employment of the schools or their role changes. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.

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

See appendix B for a sample "Checklist for Leavers" document

Access to the Council Services

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

In the school environment this currently applies to the access granted in schools to the Council's Business World finance and HR system.

Passwords

Passwords protect access to ICT systems.

All accounts with "administrator" rights should have strong passwords. The recommendation for strong passwords is a minimum of 8 characters, using a combination of upper and lower case, numbers and symbols and changed termly.

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, for example laptops which are highly portable and less physically secure.

Devices such as tablet computers, eg iPads, or smartphones should protected by a complex passcode if sensitive data accessed by or held on the device.

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

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

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

Passwords should be changed frequently to previously unused passwords. Many systems have the capability to prompt or force the user to periodically select a new password. The SIRO should decide on the appropriate duration that users could leave their password unchanged.

A typical password change frequency is termly. The interval chosen and the methods by which the password changes will be enforced must be suitably documented for users.

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

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

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

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

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

Finally, do not save passwords in web browsers if offered to do so.

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 should be taken at regular intervals as determined by the SIRO, dependent upon the importance and quantity of the data concerned. It is the responsibility of the schools and SIRO to develop a suitable backup strategy with the schools' ICT support provider.

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 schools ICT systems.

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

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

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

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

The schools 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 Shropshire ICT notifying the schools 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 irreversibly removed 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.

A sample form to record the disposal of assets is provided in appendix D.

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.

Repair of Equipment

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

System Security – Checklist

	Ensure any contractor or third party signs the form "Access to Systems by Third Parties" before access is granted
	Establish Acceptable Use Policies and ensure that these are issued to all users

	Set rules governing the use of private hardware and software
	Ensure access granted to users is sufficient
	Establish a leavers' procedure to ensure that accounts are deleted when users leave
	Enforce strong passwords where appropriate
	Ensure all school owned machines are managed so that AV and critical security updates are applied in a timely manner
	Ensure disposal is carried out in a secure manner as appropriate and that equipment disposals are recorded

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 organisations up to £0.5 million for personal data loss.

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

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

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

Personal data is any combination of data items that identifies an individual and gives specific information about them, their families or their circumstances. This includes names, contact details, gender, dates of birth, behaviour 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

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

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

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

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

Encryption

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

Data Handling – Checklist

	Appoint a Senior Risk Information Officer (SIRO)

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

Security Incidents

All suspected or actual breaches of information or ICT security, including the detection of computer viruses, must be reported to the SIRO, 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

Acceptable Use Policies for Schools – Please see our e-safety Policy

Appendix B

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

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 C

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:

Appendix D

Record of Asset Disposal Form

Record of Asset Disposal

School:

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

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

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

Details of Sale / Transfer

Has the Inventory been amended? Yes /No

Name of Certifying Officer

Signature

Date

Appendix E

Checklist for Headteachers

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

It is the Executive 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.

Checklist	
Does personal information need to be taken off site?	☐
Is the amount of personal information leaving the school limited to that which is actually needed, ie data isn't left on memory sticks or laptops if it is not specifically required?	☐
Personal data isn't stored on memory sticks or laptops unless the devices are encrypted. The Information Commissioner's Office does not consider password only protection to be sufficient.	☐
When taken out of the school, personal information is going to be kept securely and access limited to the member of staff, either in transit or in the home environment.	☐
Is anti-virus software and operating system software (Windows/Mac) kept up to date? At a minimum staff must ensure that laptops are updated as soon as they are returned to school.	☐
If school computer equipment is being taken home, access to the computer is restricted to the member of staff's usage.	☐
Personal photographs, music, video, non-school software should not be stored on a school computer.	☐
Staff are aware that they should use the computer in the home environment as they would at school, in line with any school 'appropriate usage' guidance.	☐
When the school is closed personal information and portable computer equipment remaining at school is secured out of sight.	☐
When IT users change role or leave, a Leaver's checklist is completed and their access to computer systems/devices and external websites is changed/removed accordingly.	☐

If you require any advice in relation to data protection, Freedom of Information or information security issues, please contact the Information Governance team on 01743 252774/252179.