BISHOP MARTIN C.E. PRIMARY SCHOOL

e- Safety Policy

2016-17

23/11/2016

This document incorporates the following:-

1. **Introduction**
2. **ICT Security Framework.**
3. **Data Management**
4. **E-Safety**
5. **Acceptable Use Policy (AUP)**

Appendices 1 - 10

Appendix 1 - Photographs and Images Agreement
Appendix 2 - E- safety classroom rules
Appendix 3 - ICT Security guidelines
Appendix 4 - ICT Security Rules and Agreements – Staff
Appendix 5 - E-mail and Internet Use Good Practice Rules and Agreements – Staff
Appendix 6 - Responsible E-mail and Internet Use – Staff Consent form
Appendix 7 - Acceptable Use Agreement – School Staff and Governors
Appendix 8 - Acceptable Use Agreement – Supply staff / Visitors
Appendix 9 - Acceptable Use Agreement – Pupils
Appendix 10 - Acceptable Use Agreement - Letter to Parents

This document should be read in conjunction with other Safeguarding related school policies and Reference documents.

- **School Self Evaluation Framework**
- **School Improvement Plan**
- **Staff Code of Conduct, Recruitment and Induction**
- **Anti Bullying Policy**
- **Behaviour Policy**
- **Child Protection Policy**.
- **Health & Safety Policy**
- **EYFS framework –** *Section 3.4 (2012) – Use of mobile phones and cameras*
- **Lancashire County Council ICT Security Framework for Schools**

See also: www.lancsngfl.ac.uk/esafety

Introduction

In line with the aims and principles of school values and Mission statement at Bishop Martin CE Primary school we are committed to promoting and investing in the use of ICT technology throughout the school. We recognise in many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. This policy sets out the school's approach to e-Safety along with the various procedures to be followed in the event of an incident.

E- Safety is describes as schools ability to:-

- To protect and educate pupils and staff about the benefits, risks and responsibilities of using ICT technology
- To have the appropriate mechanisms to intervene and support any incident where appropriate.

This document outlines school's ICT security framework measures, ICT Roles and responsibilities, Acceptable Use agreements for all users of school's ICT resources, the rules and agreements for safe internet and e-mail usage and guidance on the appropriate use of electronic communications such as mobile phones and wireless technology.

ICT Security Framework

The purpose of Bishop Martin CE Primary School's ICT Security framework is to protect the school's ICT information assets from all threats, internal or external, deliberate or accidental.

School's ICT security framework is based on the guidelines issues by Lancashire County Council (www.lancsngfl.ac.uk/esafety website).

It is the policy of Bishop Martin CE Primary school to ensure that:

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- ICT security training will be available to all staff

Objectives

There are three main objectives of school's ICT Security framework:

1. to ensure that equipment, data and staff are adequately protected against any action that could adversely affect the school;
2. to ensure that users are aware of and fully comply with all relevant legislation;
3. 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.
4. Undertake a 360 degree evaluation of e-safety on an annual basis.

Application

The ICT Security framework is intended for all school staff who are either controllers of the system or who are users and supporters of the school's administration and curriculum ICT systems or data.
Pupils using the school's ICT systems or data are covered by the school's 'Acceptable Use Policy' documents.

Roles and Responsibilities

Governing Body

The governing body has the 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 framework and other ICT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

Headteacher

The Head teacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's ICT Security Framework Policy, as may be amended from time to time, is adopted and maintained by the school. He/she 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.
The day to day functions are delegated to the School Business Manager who is nominated in writing by the Head teacher. This takes the form of an item in his/her job description.
The Head teacher is responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school.

In addition, the Head teacher 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 and laptops 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.

School Business Manager (nominated ICT Manager)

The School's Business Manager is the nominated ICT Manager and 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 School ICT Manager will delegate responsibility for the practical aspects of ICT protection to the school's ICT technician who will 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.

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

School ICT technician

The school technician is responsible for maintaining, repairing and proactively supporting the ICT System so that it can meet the requirements of the ICT Security Framework Policy. The School Technician will respond to actions delegated to him/her in order to ensure that the ICT System can comply with the ICT Security Policy.

The school technician will also monitor the ICT System for breaches of security and inform the nominated ICT Manager and Head teacher.

Users

Users are those employees, pupils or authorised visitors to the school who make use of the ICT system to support them in their work. All users of the school's ICT systems and data should comply with the requirements of the e-Safety this ICT Security Policy. The school has an Acceptable Use Policy which summarises the responsibilities of users of the school's ICT Systems (see Appendices 7 - 9).

Users are responsible for notifying the ICT Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Head teacher, Chair of Governors or to Lancashire County Council Internal Audit department.

Users are responsible for the equipment they use including:

- Physical security
- Security of data
- Their own passwords.
- Backing of their files/work

Pupil access

The children are supervised by staff when accessing school equipment and online materials

Training

Suitable training for all ICT users and documentation to promote the proper use of ICT systems are made available through Lancashire County Council (lpds@lancashire.gov.uk.) which include the following courses:-

- Staff Awareness sessions
- Parent e Safety briefings
- Pupil sessions
- Governor Training

Users are also given adequate information on the policies, procedures and facilities to help safeguard these systems and related data.

In addition, users are made aware of the value and importance of such ICT systems and data in particularly data of a confidential or sensitive nature, and made aware of their personal responsibilities for ICT security.

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

The Head teacher ensures that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures are applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum include:

1. 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;
2. 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 is in place;

3. a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.

Education and Training

In 21st Century society, pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The main areas of e-Safety risk that we need to consider:-

Area of Risk	**Example of Risk**
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Virus', Trojans, Spyware Premium Rate services Online gambling.
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, Cyber-tattoo, Sexting.
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact.

Security

Adequate consideration is given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons are admitted to rooms that contain servers or provide access to data and the server rooms are kept locked when left unattended.

Equipment siting

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

1. 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 is given to the siting of devices on which confidential or sensitive information is processed or retrieved;
2. equipment is sited to avoid environmental damage from causes such as dust & heat;
3. users are instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained.
4. users are instructed not to leave hard copies of sensitive data unattended on desks.

The same rules apply when accessing the School's ICT System or ICT data away from school, e.g. at a User's home or visiting another school.

Inventory

The Head teacher, in accordance with the School's Financial Regulations ensures that an inventory of all ICT equipment is maintained and all items accounted for at least annually.

Legitimate Use

The school's ICT facilities must not be used in any way that breaks the law (Misuse of Computer Act 1990) or breaches Lancashire County Council standards. Such breaches include, but are not limited to:-

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

Private Hardware & Software

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

Authorisation

Only persons authorised by the Headteacher and in full compliance with the schools ICT policies, are allowed to use the school's ICT systems. The School ICT Manager ensures the user is fully aware of the extent to which an ICT User may make use of the ICT System through school's Acceptable Use Policy (AUP).

Access eligibility is reviewed continually, including remote access for support. In particular the relevant access capability is removed when a person leaves the employment of the school. In addition, access codes, user identification codes and authorisation rules are reviewed whenever a user changes duties.

Failure to change access eligibility and passwords will leave the ICT systems vulnerable and unable to comply with the sanctions of the Computer Misuse Act 1990.

Passwords

Passwords for staff users:-

1. Encryption passwords MUST be a minimum of 8 characters, including a mix of letters (upper and lower case) and numbers.
2. Passwords should be memorised and if written down MUST not be kept with the device in any form.
3. Passwords or screen saver protection should protect access to all ICT systems. The BIOS area (basic input / output system) of ICT devices should be protected with a password to restrict unauthorised access.
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. Users must not reveal their password to anyone. The School ICT Manager should keep a log of all passwords in a secure area to which only he/she has access.

Security of the network

Only devices approved by the Head teacher are permitted to be connected to the network, either through wired or wireless connectivity.

Where devices are connected to the network using wireless, the wireless network should be secure; as a minimum this should be done using WPA. Open Access Wireless Access Points must not be connected to the school's network.

At Bishop Martin, staff must ensure they do not use pen drives to store pupil or staff details, unless authorisation from the Head teacher has been given to use an encrypted pen drive. Staff should also not store sensitive information on the hard drives of their allocated school laptop. Laptops should be password protected.

Pupil data, I.E.Ps should be saved on the school's secure network drive (P Drive) only. Should it be necessary to transfer sensitive information electronically, staff should ensure they use their Lancashire e-mail address.

Mobile devices may with permission connect to the network but in full compliance with the ICT policies and this permission may be withdrawn at any time.

Encryption

Encryption is applied to wireless networks, encryption keys should be kept secure and remain the property of the system manager and must not be shared without written permission. These are changed at least termly.

All devices that have access to data attached to the ICT System are fully encrypted

Devices subject to encryption may include:

- Laptops
- PDAs
- Smartphones/Blackberries
- USB Pen drives / Memory cards
- Desktops

Where technology prevents the use of encryption (e.g. SD Memory Cards used in Digital Cameras) then any data deemed of high risk such as images of pupils should not be stored on these devices.

Filtering of the Internet

Access to the internet for children should be filtered using an approved system. Bishop Martin uses Lightspeed (Lancashire County Council's approved filtering system).
It is the responsibility of the School ICT Manager to monitor the effectiveness of filtering at the school and report issues to the Head teacher.
Where breaches of internet filtering have occurred, the ICT Manager should inform the Head teacher and assess the risk of continued access.

Backups

In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data are taken at regular intervals determined by the School ICT Manager dependent upon the importance and quantity of the data

concerned. Backups contain data that must be protected and are clearly marked as to what they are and when they were taken. They are stored away from the system to which they relate in a restricted access fireproof location, preferably off site.

The Admin server is backed up daily remotely through RBUSS (Lancashire County Council's approved remote backup supplier). The Curriculum Server is backed up both daily and weekly by school's ICT technician using external hard drives. The weekly back up disk is stored off site. Data essential for the day to day running and management of the school is stored on the school's network.

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

Operating System Patching

The ICT manager ensures that all machines defined as part of the ICT System are patched up to date according to those releases distributed by the manufacturers of the operating systems.

Virus Protection

The school uses an appropriate Anti-virus software for all school ICT systems (Sophos)
All Users should take precautions to avoid malicious software that may destroy or corrupt data. The school will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

The school will ensure that every ICT user is aware that any device in the ICT system (PC, laptops, netbook, PDA,) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the School ICT 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.

Any third-party laptops/mobile devices and mobile storage not normally connected to the school network must be checked by the ICT technician for viruses and anti-virus software before being allowed to connect to the network.

Disposal of Equipment

The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal is to be destroyed.

Prior to the transfer or disposal of any ICT equipment the ICT 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. Bishop Martin CE Primary School uses the Lancashire County Council approved contractor for the disposal of ICT equipment.

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 school should maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

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 is considered. If data is particularly sensitive it is removed from hard disks and stored on floppy disk or other media for subsequent reinstallation, if possible. The school ensures 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.

Security Incidents

All suspected or actual breaches of ICT security shall be reported to the School ICT Manager or the Head teacher 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.

It should be recognised that the school and its staff can be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the school where insufficient action had been taken to resolve the breach.

Acceptable Use Policy

The school's Acceptable Use Policy (AUP) applies to all school staff, students and third parties who use email, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained within the AUP agreements. (see Appendices 7 - 9).

Personal Use

The School has devoted time and effort into developing the ICT Systems to assist staff with their work. It is however, recognised that there are times when you may want to use the systems for non-work related purposes, and in recognising this need the School permits you to use the systems for personal use on condition the following are applied:-

- You must not use the systems for personal use during working hours. You must not allow personal use of systems to interfere with your day to day duties. Any non-job related use of the systems during working hours may be subject to disciplinary action.
- You must not use School software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.
- Use of the systems should at all times be strictly in accordance with school's Acceptable Use policy (AUP).
- You must pay all costs should the equipment be damaged, stolen or lost when associated with personal use.
- You are responsible for any non- business related files which are stored on your school computer / laptop / iPad.

Disciplinary Implications

Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the School and the individual(s) concerned and/or civil claims for damages.

Where there is evidence of misuse or abuse that may necessitate disciplinary or possible criminal action exceptional care must be taken to maintain the integrity of any computer evidence and the following guidelines implemented

- Do not turn on or operate the subject computer, or try to access the data held on any computer media. Do not allow anyone else to touch the equipment.

- Contact Lancashire Audit Service on 01772 538400. They can advise you of the action to take and will contact the police if deemed necessary.

- If computer media is provided as evidence e.g. floppy diskettes, tapes or print outs, place it in an envelope or bag which is immediately sealed, signed and dated. This should then be stored and locked away until required by the computer investigator. Document who obtained the evidence, who secured it and who had control of it.

- Keep the number of people who know of the suspicions to a minimum – all actions taken should be kept confidential. The original suspect may have accomplices or may be innocent of the allegations.
- Do not solicit the assistance of the resident 'computer expert'. The processing of computer evidence requires specialist knowledge, training and tools.

Data management

Bishop Martin CE Primary School ensures sensitive or personal data is recorded, processed, transferred and made available for access in school in line with the requirements of the Data Protection Act 1998 (DPA) legal framework which is enforced and overseen by the Information Commissioners Office (ICO), the independent authority established to uphold information rights in the public interest and promote openness by public bodies and data privacy for individuals. This includes educational records, Head teacher's reports and any other personal information of individuals - pupils, staff and parents.

Anyone who processes personal information must comply with the eight principles of the DPA, which make sure that personal information is:

1. fairly and lawfully processed

2. processed for specific purposes

3. adequate, relevant and not excessive

4. accurate and up to date

5. not kept for longer than is necessary

6. processed in line with individuals' rights

7. secure

8. not transferred to other countries without adequate protection

All data in the school is kept secure and staff informed of what they can or can't do with data through the E- safety Policy and the Acceptable Use Policy.

Responsibilities

The Senior Leadership Team is responsible for managing information

- Staff are aware of where data is located.

- All staff with access to personal data understands their responsibilities.
- The school ensures that personal and confidential data is appropriately managed both within and outside the school environment.
- The staff are aware that they should only use approved means to access, store and dispose of confidential data
- Staff have access to school logins, to ensure the data remains secure.
- The school's policy on using mobile devices and removable media is that school confidential, personal and sensitive information is not allowed to be carried on pen drives and no school data is allowed to be removed out of school on removable devices including laptops.
- The school aims is to ensure that data loss is managed by the use of passwords for the required people.
- The school's has effective back up procedures in place.
- School's Cloud based storage provider complies with the guidelines outlined by the DFE

Bishop Martin CE Primary School wishes to confirm that it uses Microsoft OneDrive as its Cloud Based Storage Service Provider and the Head teacher confirms that they are confident of the accuracy of our supplier's self- certification statement

http://blogs.msdn.com/b/ukschools/archive/2014/10/28/microsoft-works-with-department-for-education-to-deliver-secure-cloud-services-to-schools-and-students-microsoft-office-pro-plus-benefit-currently-free-for-pupils-at-participating-schools-will-now-also-be-free-for-staff-in.aspx

Privacy Notices

Privacy Notices outline how we use information that is collated and retained by school. Privacy Notices are displayed within the school and are placed on the school's website. School holds three Privacy Notices which are as follows:-

1. Privacy Notice for Pupils

2. Privacy Notice for Children in Need or Looked After by the Local Authority

3. Privacy Notice for School Workforce

e-Safety

Vision

Bishop Martin CE Primary School provides a safe, diverse, balanced and relevant approach to the use of technology and children are encouraged to maximise the benefits and opportunities that technology has to offer:-

- Through a variety of media the children are encouraged to maximise the benefits and opportunities that technology has to offer;
- The school aims to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively;
- The children are increasingly being equipped with the skills and knowledge to use technology appropriately and responsibly;
- The school aims to recognise the risks associated with technology and how to deal with them, both within and outside the school environment;
- The users in the school community understand why there is a need for an e-Safety Policy;

The role of the Senior Leadership Team.

The role of the Senior Leadership Team and e-Safety co-ordinator include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's e-Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an e-Safety incident occur.
- Ensuring the e-Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with e-Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging e-Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head teacher, SLT, staff, pupils and Governors are updated as necessary.
- Liaising closely with the school's Designated Senior Leader / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

Use of mobile devices

Bishop Martin CE Primary school recognises that the use of mobile devices offers a range of opportunities to extend children's learning. These include laptops, cameras, iPads. These can pose challenges in terms of e-safety. Staff are made aware of the Acceptable Use Policy in respect of any mobile device. They are made aware that mobile devices can be used for cyberbullying and safeguarding procedures should be followed to minimise this from happening. They are also made aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content and many of these devices integrate functionality to take images, access the internet and engage users in various methods of external communication. Visitors are monitored for any covert use of mobile phones/cameras.

The following procedures have been implemented:-

- Mobile devices are not encouraged to be brought into school by children. If a device is brought in by mistake or is needed after school, the children are asked to hand it into their teacher or be taken to the office.

- Mobile phones can only be used within school during the school day by staff and visitors in the event of an emergency, at lunchtime or break time and must be switched off or on silent during the school day.

- Mobile phones cannot be used in changing areas or toilets.

- Access to the Internet via school's mobile devices is only allowed through School's wi fi connection. This access is controlled and filtered via Lancashire County Council's Lightspeed filtering system.

- It is acceptable to use personal mobile phones for school activities e.g. school trips.

Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure or display.

At school, photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), and the school has written permission for their use from the individual and/or their parents or carers (see Appendix 1).

- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used;
- The parental/carer permission is obtained in reception but the parents have a right to change this if deemed necessary;
- The staff and pupils ae made aware that full names and personal details will not be used on any digital media, particularly in association with photographs;
- Parents/carers, who have been invited to attend school events are not allowed to take videos and photographs;
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites;
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes;
- The school ensures that any photographs/videos are only accessible to the appropriate Staff / pupils;
- Staff are encouraged not to store digital content on personal equipment;
- The staff are encouraged not to use their own cameras;
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted;
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved;
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the S.L.T and Governors on an annual basis.

Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

- All users have access to the Lancashire Grid for Learning service as the preferred school email system.
- Only official email addresses are used between staff and with pupils/parents when Personal / sensitive data is involved.
- The Lancashire Grid for Learning filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Lancashire County Councils IT department.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- All users are encouraged to include a standard disclaimer at the bottom of all outgoing emails (see below).

****

This e-mail is confidential and privileged. If you are not the intended

recipient do not disclose, copy or distribute information in this e-mail
or take any action in reliance on its content.
****
This email has been checked for known viruses.

- Whole-class or group e-mail addresses will be used.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Internet

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

The internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Benefits

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as the National Grid for Learning (NGFL) and the Virtual Teacher Centre (VTC);
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LEA and DCSF.

School Internet Access

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval, and safe usage.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Internet Access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupils' access.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional direct supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access.

Staff Use

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school (see Appendix 6).
- All staff including teachers, classroom assistants and support staff, will be provided with access to the School Internet Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in the safe and responsible Internet use and on school Internet policy will be provided as required.

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook and Twitter. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.

All staff are made aware of the following points:-

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils must not be added as 'friends' on any Social Network site.
- Children who are under 13 are not legally allowed to be members of Facebook.
- The content posted online should not: bring the school into disrepute, lead to valid parental complaints, be deemed as derogatory towards the school and / or its employees, be deemed derogatory towards pupils and / or parents, bring into question their appropriateness to work with children and young people.
- Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Chat rooms

- Pupils will not be allowed access to chat rooms.

- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

Instant Messaging or VOIP

Instant messaging systems e.g text messaging, Skype, Facetime are popular communication tools with adults and children. They can provide an opportunity to communicate in real time using text, sound and video. The Lancashire Grid for Learning filtering service blocks some of these sites but access can be changed at the request of the Head teacher.

School ensures the following:-

- Staff and children are made aware of the risks involved using this technology e.g viewing inappropriate images or making unsuitable contacts.

Virtual Learning Environment (VLE) / Learning Platform

Bishop Martin CE Primary School uses various VLE / Learning platforms such Sumdog, Bug Club as a communication. The following guidance should be adhered to:-

- All children will be given access to the VLE but SLT have access to all accounts
- Passwords are issued to the children and they are encouraged not to share their password
- Pupils are taught to use these communication tools in a responsible way in conjunction with the e-Safety curriculum.
- Teachers know how to monitor the use of VLE's with their class.
- Accounts are deleted when staff and pupils leave the school. This is monitored by the SLT

Web sites and other online publications

This may include for example, podcasts, videos and blogs.

The school website is effective in communicating e-Safety messages to parents/carers and regularly updates the Internet and e-Safety Pupil / Parents guidance section.

- Everybody in the school is made aware of the guidance for the use of digital media on the website.
- Everybody in the school is aware of the guidance regarding personal information on the website.
- Teachers have access to edit the school website.
- The Head teacher has overall responsibility for what appears on the website.
- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The Head teacher or nominee will take overall editorial responsibility and ensure content as accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Others

The School will adapt/update the e-Safety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication.

Dealing with incidents

At Bishop Martin an incident log is completed to record and monitor offences. This is audited on a regular basis by the Senior Leadership Team.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.

It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to the Internet Watch Foundation (http://www.iwf.org.uk).

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website http://www.iwf.org.uk

Inappropriate use

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the action and control measures to be applied.

Some examples of inappropriate incidents are listed below with suggested action.

Incident	**Procedure and Sanctions**
Accidental access to inappropriate materials.	• Minimise the webpage/ Turn the monitor off. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform SLT or designated e-Safety coordinator who are responsible for dealing with incidents. • Enter the details in the Incident Log. • Additional awareness raising of
Deliberate searching for inappropriate materials	

Bringing inappropriate electronic files from home.	e-Safety issues and the AUP with individual child/class • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.
Using chats and forums in an inappropriate way.	

.

- All staff are aware of the different types of e-Safety incident and how to respond appropriately e.g. illegal or inappropriate.
- Children are informed of the procedures through discussions with members of staff.
- These incidents are logged in a log book kept in the office.
- Incidents are monitored, by the SLT on a regular basis.
- The measures that are in place to respond to and prevent recurrence of an incident.
- The SLT will decide at which point parents or external agencies are involved

The procedures are in place to protect staff and escalate a suspected incident/allegation involving a staff member.

e-Safety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own e-Safety. Bishop Martin provides suitable e-Safety education to all pupils:

- Regular, planned e-Safety teaching within a range of curriculum areas (using the Lancashire ICT Progression framework)
- E-Safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- The school ensures that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, e-Safety rules (see Appendix 2).

e-Safety – Raising staff awareness

- Formal training is available for staff to ensure they are regularly updated on their responsibilities as outlined in our school policy.
- The e-Safety co-ordinator (IT subject leader) provides advice/guidance or training to individuals as and when required.
- The e-Safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources
- E-safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's e-Safety Policy and Acceptable Use Policy.
- Guidance notes on Acceptable Use, ICT Security, E-mail and Internet Rules are made available for staff (see Appendices 3 - 5).
- Regular updates on e-Safety Policy, Acceptable Use Policy, curriculum resources and general e-Safety issues are discussed in staff/team meetings.

e-Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come

across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

The school offers opportunities for parents/carers and the wider community to be informed about e-Safety, including the benefits and risks of using various technologies. For example through:

- School newsletters, homework diaries, Website, VLE and other publications.
- Promotion of external e-Safety resources/online materials is made available on the school website..

e-Safety – Raising Governors' awareness

The school considers how Governors, particularly those with specific responsibilities for e-Safety, ICT or child protection, are kept up to date. This is through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

The ICT Security policy incorporating the e-Safety Policy will be reviewed yearly (and/or if a serious breach occurs) by the e-Safety coordinator, approved by the governing body and made available on the school's website.

Inspection and Evaluation

Bishop Martin CE Primary school evaluates the impact of safeguarding procedures within the school's e-safety policy by the following means:-

- E-Safety incidents are monitored, recorded and reviewed.
- The SLT are responsible for monitoring, recording and reviewing incidents.
- The introduction of new technologies is risk assessed.
- These assessments are included in the e-Safety Policy.
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children.
- These patterns would be addressed most effectively by e.g. working with a specific group, class assemblies, reminders for parents.

<u>Risk Assessment</u>

- The school will take all reasonable precautions to ensure that users access only appropriate material through using a filtering system. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school or LCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher or nominee will ensure that the Internet policy is implemented and compliance with the policy monitored.

<u>Complaints</u>

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaints about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

<u>Parents</u>

- Parents' attention will be drawn to the School Internet Policy

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Acceptable Use Policy (AUP)

Bishop Martin CE Primary School has a responsibility to inform all users of school's ICT technology about the type of behaviour it expects an about the consequences for abusing ICT technology privileges. The Acceptable Use Policy (AUP) is intended to ensure that all users of technology within school will be responsible and stay safe. The AUP agreements (see Appendix 7 - 9) provide this information to users of the school's ICT resources whether they are members of staff, volunteers, supply staff or pupils.
AUPs are used for Staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.

Our school AUPS aim to:-

- Be understood by the each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the e-Safety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
- Cyberbullying
- Inappropriate use of email, communication technologies and Social Network sites
- and any online content
- Acceptable behaviour when using school equipment /accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of e-Safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

Appendix 1

BISHOP MARTIN CE PRIMARY SCHOOL – PHOTOGRAPHIC & VIDEO IMAGES

Please read through this letter and keep this copy at home

Bishop Martin CE Primary school will do all it can to ensure that images are used properly, and that, as in all matters, risks are minimised, and our children kept safe and secure, whether at school or elsewhere. The aim is to establish the right balance between the proper use of technology and the safety of our children at all times.
No image is used for display or for school publicity etc., unless consent is given by the parent or carer of the individual concerned

Parental permission
All parents and carers will be asked to sign a consent form allowing their child to be photographed or videoed while taking part in school activities, such as sports events, drama productions, field trips, etc., and for the school to use these pictures internally within the school. This form will be given to the parents or guardians of all children joining the school in each successive year. Where parents or carers do not give their consent, then the children concerned will not have pictures taken of them.
All pictures taken will be appropriate, and will show children properly clothed for the activity they are engaged in. The school will do all it can to ensure that due sensitivity is shown in the choice and composition of these images.

School performances
We will allow video and photographic recordings of all school performances, as long as the parents or guardians of the children involved have given their consent.
The school will observe the way in which video recordings are made, and photographs taken, during performances, and will withdraw the right of anyone to bring a camera of any sort if they are felt to be making inappropriate images. For example, photography is forbidden in changing rooms or backstage during school productions.

The Internet
Only appropriate images will be used on the school internet site, and children will not be identified by their name or address on the school website.

Mobile phones
We do not allow children to bring mobile phones into school. Staff may bring mobile phones, but must not use them to take pictures of children.

Use of digital cameras
There are many ways in which the use of digital images is valuable for children's learning. For example, they may be used in art work or geography or science fieldwork. In Foundation Stage photographs are often taken to exemplify and assess children's 'Learning Journey'. Images will be made only as appropriate for school-related activities.
Children will be taught how to take pictures, but we will discourage them from taking pictures of each other, and they will be supervised by an adult when they have access to a digital camera.
As soon as images have been used for their intended purpose (e.g. illustrating a good football pass) they will be deleted. The school will not store digital images any longer than for their immediate use.

Media publications
Sometimes, local or national media visit the school to follow up a news story. This is often to do with a notable achievement by a child or a group of children from the school. In this situation, where children's images might be made public, the school will inform parents and carers of the event in advance, and allow them to withdraw their child from the event if they so wish. Newspapers normally ask for the names of the children to go alongside the photographs; if parents or carers do not wish this to happen, then the school will not allow the individual to be photographed or filmed by the media concerned.

BISHOP MARTIN CE PRIMARY SCHOOL

PHOTOGRAPHIC & VIDEO IMAGES SAFETY AGREEMENT - SCHOOL COPY

- Bishop Martin CE Primary School will do all it can to ensure images are used properly and no image is used for display or for publicity etc. unless consent is given by the parent or guardian. Any child will not be directly identified.

- Only appropriate images will be used on the school internet site and children will not be identified by their name or address on the school website.

- Pupils are not allowed to bring mobile phones into school. Staff may bring mobile phones, but must not use them to take pictures of children.

- Bishop Martin will only allow video and photographic recordings of school performances as long as the parents or guardians of the children involved have given their consent. The School will withdraw the right of anyone to bring a camera of any sort if they are felt to be making inappropriate images.

- Digital cameras can only be used for recording images of school related activities to support children's learning for example artwork, geography. In Foundation Stage photographs are taken to exemplify and assess Children's 'Learning Journey'. Pupils will be taught how to take pictures and supervised at all times when they have access to a digital camera As soon as images have been used for their intended purpose, they will be deleted. The school will not store digital images any longer than their immediate use.

- Bishop Martin will inform parents or guardians in advance, if the media intend to visit the school to record a school event. The media normally ask for names of the children to go alongside photographs; if parents do not wish this to happen, they can withdraw their child from the event if they so wish.

PARENTS CONSENT FOR USE OF IMAGE OF PUPILS

I have read through this agreement and understand the safety restrictions.

CHILDS NAME_____ **CLASS**_____

Subject to the rule that photographs and images will not clearly identify individuals and that full names are not used**, I give permission** for the school to use;

- My child's photograph in publications such as the School prospectus, promotional materials
- My child's image on the school website.
- My child's image to be recorded on video/CD at school performances or events.
- My child to appear in the media as part of the school's involvement in an event.

PARENTS / GUARDIANS signature _____ **Date:** _____

Appendix 2

eSafety Rules (EYFS/KS1)

Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

eSafety Rules (KS2)

Golden Rules for Staying Safe with ICT

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell a trusted adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programs and content which have been installed by the school.

Appendix 3

BISHOP MARTIN C. of E. PRIMARY SCHOOL

ICT Security Guidelines

1. Password Policy

Passwords should be:

- unique
- alphanumeric
- at least 6 digits in length
- regularly changed, recommend at least every 90 days

Passwords should NOT be:

- written down
- easy to guess, don't use family or pet names for example

2. Monitoring Computer Use by Pupils

- Ensure Pupil use of computers is 'visual', make sure there is a Teacher present and monitoring use
- Consider logging access to the network using software tools, for example RM 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
- 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, floppy disks, computers etc. that may contain sensitive or personal information.
- Floppy discs or pen drives should not be used to store sensitive or personal information e.g pupil details, IEPs. Authorisation may be given by the Headteacher to use encrypted pen drives in exceptional circumstances.

4. System Backup

- The system is backed up regularly by an automated system.

5. Anti Virus Protection

- Approved and recommended product is used.
- Assistance will be sought from LCC or MC3 when dealing with any actual or suspected infections

6. Illegal or Inappropriate Use of the Network

- Auditing is performed both at the Management System level and also at the Operating System level.
- LCC firewall is in place to restrict external activity and access.

7. Internet Use / Filtering

- School Internet policy has been adopted and staff are required to signed up to it.
- Parental permission is obtained.
- Internet use is supervised

8. Email Use

- Staff should use their secure Lancashire e-mail address when transferring sensitive data and personal information, in particular pupil details, IEPs, pupil reports etc. Staff should limit the use of personal e-mail addresses.

9. Training

- There is adequate training for System Managers and Users
- 'Good practice' guidelines where appropriate e.g. using screen savers with passwords are made available

10. Authentication / Operating System Level Security

- There is a rigorous policy for approval / removal of Users
- The use of 'generic' accounts is avoided
- 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
- Consider using 'read only' access where possible

11. Review

- School policies will be reviewed on an annual basis or as appropriate.
- Review procedures for dealing with all security breaches or compromises, whether deliberate or innocent

Appendix 4

BISHOP MARTIN C. of E. PRIMARY SCHOOL

ICT Security Rules and Agreements for Staff

- Ensure you know who is in charge of the ICT system you use, i.e. the System Manager.

- 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

  Provisions of this legislation may result in disciplinary, civil and/or criminal action.

- 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.

- 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 with the terms of its licence and may only be copied if specifically approved by the System Manager.

- 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 your 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.

- You must not exceed any access rights to systems or limitations on the use of data granted to you by the System Manager.

- The ICT 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 8 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.

- The ICT 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.

- 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.

- Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, floppy disks, etc.

- 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 ICT Manager or the Headteacher, , in exceptional cases, Chair of Governors or Internal Audit.

- Users of these facilities must complete the declaration for Responsible E-mail and Internet Use and the appropriate Acceptable Use Policy agreement.

Appendix 5

BISHOP MARTIN C. of E. PRIMARY SCHOOL

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

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;

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.

Appendix 6

BISHOP MARTIN C. of E. PRIMARY SCHOOL

Staff Consent Form

Responsible E-mail and Internet Use Please complete, sign and return to the School Business Manager	
Name:	
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:

Appendix 7

BISHOP MARTIN C. of E. PRIMARY SCHOOL

ICT Acceptable Use Policy - Staff and Governor Agreement

ICT and the related technologies such as email, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head teacher.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will be an active participant in e-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
- I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
- I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I will ensure that all electronic communications with pupils and other adults are appropriate.
- I will not use the school system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes.)
- I will not install any hardware or software without the prior permission of the SLT
- I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
- I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- I will report any known misuses of technology, including the unacceptable behaviours of others.
- I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
- I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.
- I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
- I will take responsibility for reading and upholding the standards laid out in the AUP. I will
- support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..…….…… Date ……..……..……
Full Name
……..……
…… (PRINT)
Position/Role
……..……...…….

Appendix 8

BISHOP MARTIN C. of E. PRIMARY SCHOOL

ICT Acceptable Use Policy - Supply teachers and Visitors/Guests Agreement

For use with any adult working in the school for a short period of time.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto any school system.
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..…… Date ……..……
Full Name
……..……..…….
…… (PRINT)
Position/Role
……..……...…….

Appendix 9

BISHOP MARTIN C. of E. PRIMARY SCHOOL

ICT Acceptable Use Policy - Pupils Agreement / eSafety Rules

These rules are a reflection of the content of our school's e-Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- I will only use ICT in school for school purposes.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class email address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others' details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

……

Parent/ Carer signature

We have discussed this Acceptable Use Policy and
…….....
[Print child's name] agrees to follow the e-Safety rules and to support the safe use of ICT at Bishop Martin C.E. School.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Class …….. Date……

Appendix 10

BISHOP MARTIN C. of E. PRIMARY SCHOOL

ICT Acceptable Use Policy (AUP) – Parents' Letter

<Insert School's Letterhead>

Dear Parent/ Carer,
The use of ICT including the Internet, email, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within and outside of, the school environment.
This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites do have age restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School e-Safety Policy and alongside the school's Behaviour Policy outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community.
Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.
If you would like to find out more about e-Safety for parents and carers, please visit the Lancsngfl e-Safety website http://www.lancsngfl.ac.uk/esafety

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school.
If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact the school office.

Please read through this letter and keep this copy at home.