Ivington C of E Primary and Pre-school

Reaching together… 'stand firm in your faith, be courageous and strong' – 1 Corinthians 16:13

E - Security Policy

Approval of the Governing Body

This document is a statement of the aims, principles and strategies for:

E-Security Policy

at

Ivington CE (VA) Primary and Pre-school

It was revised during the:

Summer 2023

It has been agreed and is supported by the teaching staff and the governing body.

We aim to review this policy during the:

Summer 2025
Or sooner if necessary

Linking with our Vision

To provide a caring, Christian ethos for the school, which inspires and excites a shared enthusiasm for life and learning.

At Ivington CE Primary and Pre-school, through our strong Christian ethos and focus on 12 important Christian values, we are committed to providing a deeply nourishing, spiritual, ambitious, and broad curriculum. Our motto, 'Reaching together' underpins our belief in equality of opportunity for all, where we actively endeavour to promote understanding and appreciation of our racially diverse society and give each child a special place in the world where they feel valued, essential to our community and equipped with the necessary skills to make a positive contribution. We perceive our role to be opening a 'window on the World', through which our pupils are actively encouraged to develop respect for the beliefs and cultures which enrich their everyday lives and encourage others to do likewise.

We strive to eliminate inequality through our deep Christian ethos of tolerance and understanding of all groups in society, which ensures that everyone at Ivington will be treated fairly despite his or her creed, colour, disability, or gender.

More details are available in our Inclusion, Racial Equality and Equal Opportunities policies.

The health, safety, and welfare of all the people who work or learn at our school are therefore of fundamental importance. We aim to provide a safe, secure, and pleasant working environment for everyone. The governing body, along with the LA, takes responsibility for protecting the health, safety and welfare of all children and members of staff.

Background and rationale

Recent publicity about the loss of personal data by organisations and individuals has made e-security a current and high profile issue for schools and other organisations. It is important that schools have a clear and well-understood policy on e-security because:

- No school or individual would want to be the cause of any loss of personal data, particularly as the impact of data loss on individuals could be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The school will want to avoid the criticism and negative publicity that could be generated by any loss of personal data.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but from remote locations. The UK Data Protection Act 1998 addresses legislation covering the safe handling of this data and following a number of losses of sensitive data, the Cabinet Office in June 2008, Data Handling Procedures in Government published a report. This stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that they adopt these procedures too.

It is important to stress that the policies relating to personal data apply to all forms of that data, regardless of whether it is held on paper or in electronic format. As it is part of an overall e-safety / e-security policy template, this document will place particular emphasis on data which is held or transferred digitally and on the security of systems and technology that hold that data.

Section A – Personal data security

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed. Data within the SIMS System will be retained throughout the life of the system pupil details MUST NOT be deleted, the school is responsible for retaining pupil records in line with County Policy.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

This should be read alongside the school Data Protection Policy.

A.1 Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

A.2 Responsibilities

The school's Senior Risk Information Officer (SIRO) will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand :

- what information is held and for what purpose
- how information as been amended or added to over time
- who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

A.3 Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

A.4 Information to parents/carers – the "Fair Processing Notice"

Under the "Fair Processing" requirements in the Data Protection Act, the school will inform parents / carers of all pupils of the data they hold on the pupils, the purposes for which the data is held and the third parties (eg LA, DfE, Connexions etc) to whom it may be passed. This fair processing notice will be passed to parents / carers through ... Parents / carers of young people who are new to the school will be provided with the fair processing notice through. It is also possible for the school to provide parents / carers with a data collection sheet for checking / retaining that will show all personal data held for the pupil.

A.5 Training & awareness

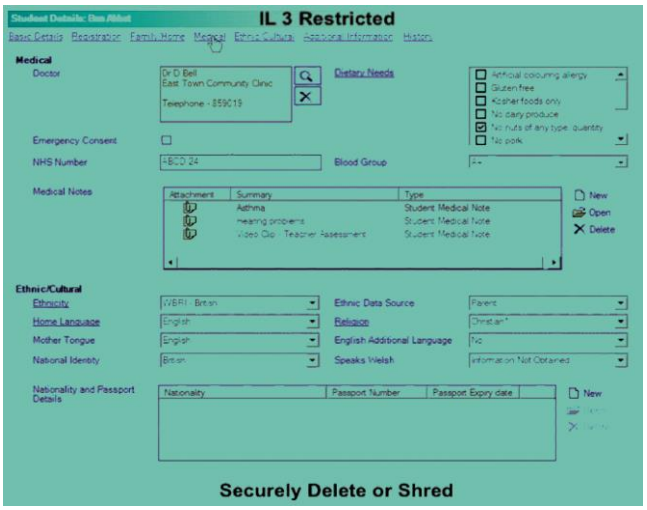
All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners.

A.6 Identification of data

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents (manual or digital) that contain protected data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer:



Impact levels are as follows:

- IL1–Not Protectively Marked (IL1–NPM)
- IL2–Protect
- IL3–Restricted
- IL4–Confidential

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data.

Release and destruction markings will be shown in the footer as follows:

[Release]	**[Parties]**	**[Restrictions]**	**[Encrypt, Securely delete or shred]**
The authority descriptor	The individuals or organisations the information may be released to	Descriptor tailored to the specific individual	How the document should be destroyed
Examples:			
Senior Information Risk Owner	School use only	No internet access No photos	Securely delete or shred
Teacher	Mother only	No information to father ASBO	Securely delete or shred

A.7 Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Schools set the access rights for their staff from a prescribed menu within SIMS however these 'roles' are editable by the school.

All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data is not to be stored on school equipment (this includes computers and portable storage media). Private equipment (ie owned by the users) must not be used.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected (Please see backup documentation from the local authority (revised September 2011)

- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

A.8 Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Anycomms and Anycomms + are currently used by Herefordshire schools for the secure transfer of data, Our school does not email pupil data.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

A.9 Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

A.10 Audit Logging / Reporting / Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Section B - Password security

The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

B.1 Policy Statements

All users (at KS2 and above) will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the *ICT Technician* and will be reviewed, at least annually, by the E-Safety Committee *(or other group).*

All users (at KS2 and above) will be provided with a username and password by the school's *ICT Technician* who will keep an up to date record of users and their usernames and has the ability to reset passwords.

Pupils in EYFS and KS1 do not usually use their individual logins, simple class logins are used instead (though every pupil's individual login is available and ready to be used at any time and children in Y2 especially are often moved on when it is felt they are ready for this).

Users are not routinely required to change their passwords, though the school's e-safety education programme makes clear the advantages of doing so and especially where high security is important. Users are required to change their passwords themselves if their details become known by another person. Class passwords (below KS2) are not changed.

Staff users have the facility to access all pupil work areas via their normal login. This is to enable monitoring of work and ICT activity by children.

This is also useful in the situation where a pair or group of children have been working collaboratively and the child whose login was used is unexpectedly absent; the teacher can move the work in question to another child's work area. In this way it is not necessary for a child to login using another child's account.

A multi-user account is available for visitors to the school (e.g. supply teachers). This has been carefully controlled to give only the access to the system that is needed and the username and password is given to users as required.

In the extraordinary case of a member of the wider community needing access to the school's ICT system outside the normal work of the school (e.g. for out of hours use by a community group) a special login is created by the school's ICT Technician with access rights agreed with the head teacher, ICT coordinator or e-safety coordinator. Such users are required to sign an Acceptable Use Policy (see Appendix 1 of the e-safety policy) before being granted this access.

Encryption software is installed on all staff laptops (where potentially sensitive data is stored and the machines are regularly taken off site).

The "master / administrator" passwords for the school ICT system, used by the Network Manager and usually also the ICT coordinator must also be available to the head teacher or other nominated senior leader and kept in a secure place (eg school safe). (Alternatively, where the system allows more than one "master / administrator" log-on, the head teacher or other nominated senior leader should be allocated those master / administrator rights. A school should never allow one user to have sole administrator access).

B.2 Responsibilities

The ICT technician will be responsible for the day to day management of the password security policy

All users (adults and young people other than pupils in EYFS and KS1) will have responsibility for the security of their username and password. They:

- must not allow other users to access the systems using their log on details and
- must immediately report any suspicion or evidence that there has been a breach of security
- must change their password if they are aware that it has become known by another user.
- must logoff at the end of their session and before leaving the computer.

EYFS and KS1 pupils use class logins which are shared.

Passwords for new users, and replacement passwords for existing users can be allocated by the ICT technician or, if needed more immediately, the ICT coordinator .

Any changes carried out to passwords must be notified to the manager of the password security policy (above).

B.3 Training and awareness raising

We recognise that is important that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. Please see section C of the school's e-safety policy for specific guidance on e-safety education (which includes the use of passwords)

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety and e-security policies
- through the Acceptable Use Agreement (see Appendix 1 of the school e-safety policy)

Pupils will be made aware of the school's password policy:

- in ICT and / or e-safety lessons (the school should describe how this will take place)
- through the Acceptable Use Agreement (see Appendix 1 of the school e-safety policy)

B.4 Audit, monitoring, reporting and review of password policy

The responsible *person (insert title)* will ensure that full records are kept of:

- User IDs and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed at regular intervals.

This policy will be regularly reviewed (along with the e-safety policy) on a regular basis (see section A.2.1 of the e-safety policy) and in response to changes in guidance and evidence gained from the logs.

Section C - Technical security

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-security responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the schools e-safety and e-security policies and acceptable use policy and in line with the policies of Herefordshire ICT Services (to whose infrastructure the school is connected)
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

The school infrastructure and individual workstations are protected by up to date virus software.

Pupil accounts allow access to limited storage areas, they cannon access local hard drives and are unable to run executable files.

Staff accounts allow greater access to the network and to local drives. Staff are able to run executable files but do so within the acceptable use agreement they sign (see Appendix 1 of the e-safety policy)

Staff laptops are provided for staff professional use while the member of staff is employed by the school.

- *These machines are allowed off-site and are protected by encryption software*
- *Members of staff are permitted to install software on these machines as long as the installation is legal, within the scope of the licensing agreement owned by the school and professionally necessary.*
- *The storage of personal files (including image, music and video collections) on computers owned by the school is not permitted.*
- *Members of staff are not permitted to store school data on personally owned devices.*

Please refer to section A.2.6 of the e-safety policy for definitions of inappropriate or illegal activity and related sanctions.

Please refer to the sections in A.3 of the e-safety policy for further guidance on acceptable use.

Appendix 1 – Legislation

Schools should be aware of the legislative framework under which this E-Security Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. Please see Appendix 1

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Appendix 2 - Supporting resources and links

Teachernet – Data processing and sharing - http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/

Office of the Information Commissioner website: http://www.informationcommissioner.gov.uk

Office of the Information Commissioner – guidance notes: Access to pupil's information held by schools in England

Information Commissioners Office - Data Protection: http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

Becta – Good Practice in information handling in schools – keeping data secure, safe and legal and its four detailed appendices: (September 2008)

Please note that the Becta website is now archived at: http://webarchive.nationalarchives.gov.uk/20110130111510/http:/www.becta.org.uk

Cabinet Office – Data handing procedures in Government – a final report (June 2008)

http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

South West Grid for Learning "SWGfL Safe" http://www.swgfl.org.uk/safety/default.asp

InSafe http://www.saferinternet.org/ww/en/pub/insafe/index.htm

Byron Review ("Safer Children in a Digital World") http://www.dcsf.gov.uk/byronreview/

London Grid for Learning http://cms.lgfl.net/web/lgfl/365

National Education Network NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

WMNet – www.wmnet.org.uk

Appendix 3 - Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are still used)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
DfE	Department for Education
FOSI	Family Online Safety Institute
HSCB	Herefordshire Safeguarding Children Board (the local safeguarding board)
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by Becta
ICT Services	Herefordshire ICT Services - provide broadband services and ICT support to Herefordshire schools
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider

IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1 ..	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
LA	Local Authority
LAN	Local Area Network
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SRF	Self Review Framework – a tool maintained by Naace used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to e-safety (on whose policy this one is based)
URL	Universal Resource Locator – posh name for a web address
VLE	Virtual Learning Environment - an online system designed to support teaching and learning in an educational setting,
WMNet	The Regional Broadband Consortium of West Midland Local Authorities – provides support for all schools in the region and connects them all to the National Education Network (Internet)