Much Birch C of E Primary School

Online Safety Policy



'We will flourish and reach our God given potential'

I am the vine; you are the branches. If you remain in me and I in you, you will bear much fruit. **John 15:5**

All members of our whole school community are able to realise their God-given potential, enabling them to become equal, caring and active citizens whilst upholding true Christian values. We treat others, as we would like to be treated, with dignity and respect. Everyone is encouraged to flourish with hope and high aspirations

Updated:	2 Yearly
Review date:	January 2027
Head teacher:	Mrs. B. Davies
Chair of Governors:	Rev Mark Johnson

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably truer for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn.

At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology **while they are in school**.

We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks.

We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our school's e-safeguarding policy has been written from a template provided by Herefordshire Council's Learning and Achievement Service which has itself been derived from that provided by the South West Grid for Learning.

Section A - Policy and leadership

This section begins with an outline of the **key people responsible** for developing our Online Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**

A.1.1 Responsibilities:

Our senior leadership team are the people responsible for the day to day issues relating to e-safety.

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments agree timeframe
- receives appropriate training and support to fulfil their role effectively
- has responsibility for blocking / unblocking internet sites in the school's filtering system / passing on requests for blocking / un blocking to the ICT Helpdesk (see section B.2.1)
- maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices (see section A.2.8)

A.1.2 Responsibilities: executive head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the ICT lead / Deputy
- The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in section 2.6 below and relevant Local Authority HR / disciplinary procedures)

A.1.3 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they report any suspected misuse or problem to the ICT lead / Deputy
- digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems (see A.3.5)
- online safety issues are embedded in the curriculum and other school activities (see section C)

A.1.4 Responsibilities: ICT technician (John Finch Computers)

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- the school meets the online safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority Online safety Policy and guidance (NOTE: The HSCB Online safety Policy is currently under review and not presently available (October 2011)
- users may only access the school's networks through a properly enforced password protection policy as outlined in section B.1 of this policy
- short-comings in the infrastructure are reported to the head teacher so that appropriate action may be taken.

A.2.1 Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

A.2.3 Self Evaluation

Evaluation of online safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers …) are taken into account as a part of this process.

A.2.4 Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core Computing policies

Computing Policy	*How ICT is used, managed, resourced and supported in our school*
Online safety Policy	*How we strive to ensure that all individuals in school stay safe while using ICT. The online safety policy constitutes a part of the ICT policy.*
Social Media Policy	*How we implement and use social media within our school.*

Other policies relating to e-safety

Behaviour	*How our school deals with cyber bullying in school*
PSHE	*Online safety has links to this – staying safe*
Safeguarding	*Safeguarding children electronically is an important aspect of E-Safety. The online safety policy forms a part of the school's safeguarding policy*

A.2.5 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**

- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

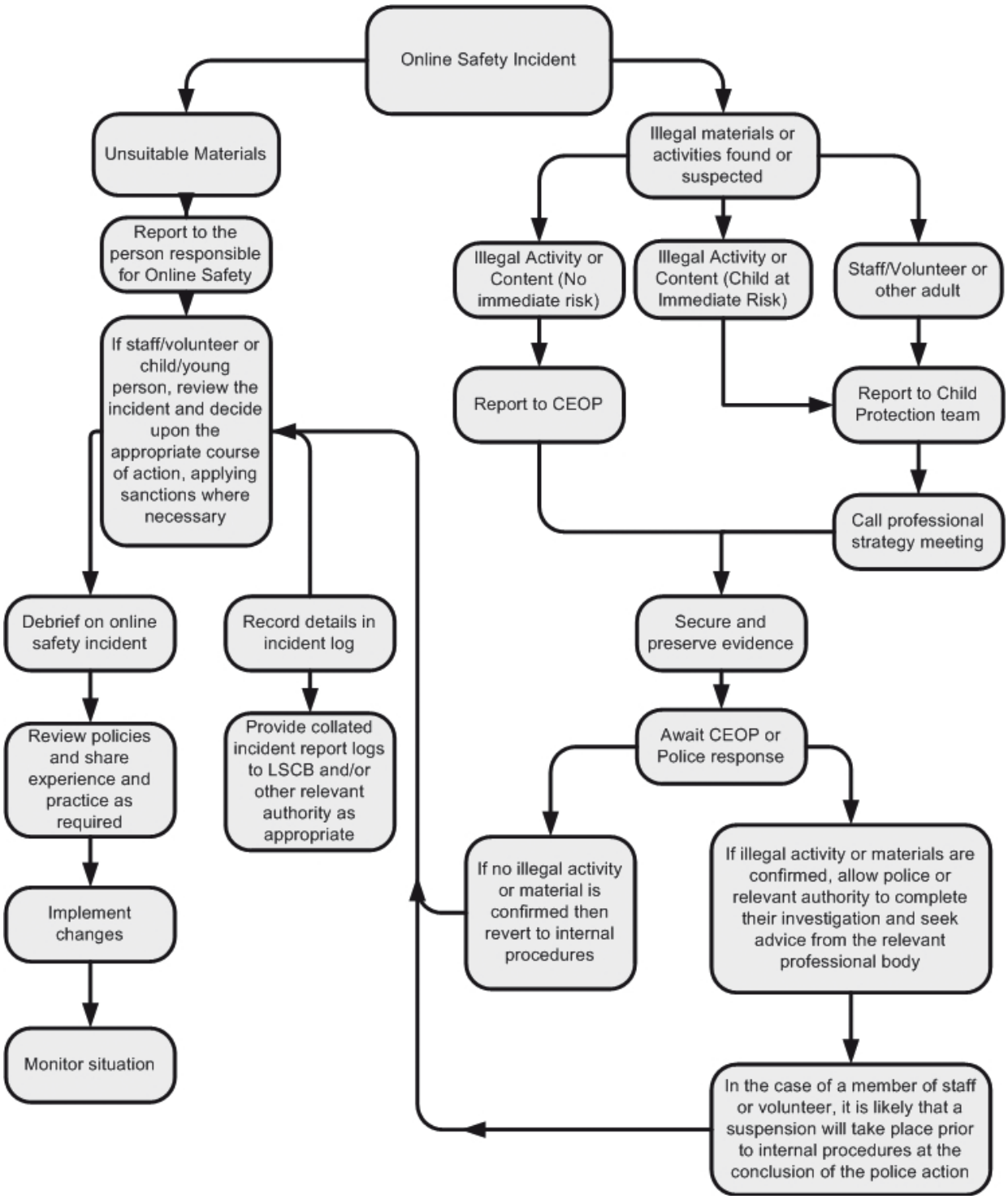
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Herefordshire Council and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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 as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

A.2.6 Reporting of online safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse: Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.6 of this policy



Responsibilities

The Head teacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: **John Finch Computers**

The Head teacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training / Awareness

Members of staff authorised by the Head teacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Our search policy

This Online safety Policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

The school's policy on the use of mobile devices is set out in section A.3.1 of this policy and the sanctions relating to breaches of these rules in section A.2.6

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or files on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- **Searching with consent** - Authorised staff may search with the pupil's consent for any item.
- **Searching without consent** - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:

- The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.
- There is a limited exception to this rule: authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

- The person conducting the search may not require the pupil to remove any clothing other than outer clothing.
    - Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
- A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
    - 'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

- The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.
- Use of force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Audit / Monitoring / Reporting / Review

The Online safety coordinator will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the head teacher / and a governor on a termly basis.

A.3.1 Use of hand held technology (personal phones and hand held devices)

- Please see our mobile phone policy

A.3.2 Use of communication technologies

A.3.2a - Email

Access to email is provided for all users in school via the intranet page accessible via the web browser (internet Explorer) from their desktop.

In addition messaging (and email for staff) is available through the Herefordshire its learning VLE

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (eg by remote access).

- Users need to be aware that email communications may be monitored
- Pupils normally use only a class email account to communicate with people outside school and with the permission / guidance of their class teacher.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- Staff do use their own personal email accounts on school systems.
- Users must immediately report, to their class teacher / online safety coordinator – in accordance with the school policy (see sections A.2.6 and A.2.7 of this policy), the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

A.3.2b - Social networking

See Social Media policy.

A.3.2c - Videoconferencing

Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.

Equipment connected to the National Education Network (NEN) should use the national E.164 numbering system and display their H323 ID name.

External IP addresses should not be made available to other sites.

Videoconferencing contact information should not be put on the school Website.

Only web based conferencing products that are authorised by the school are permitted for classroom use.

All videoconferencing is supervised by a teacher.

Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in schools) and only where it is granted may children participate.

Only key administrators have access to videoconferencing administration areas.

Unique log on and password details for the educational videoconferencing services (such as the Janet booking system) are only issued to members of staff.

Zoom or TEAMS is used in school for small group video conferences. The following safeguards are in place:

- The Zoom client software is installed only on selected computers
- The use of Zoom with children is at all times monitored by staff

A.3.3 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section (A.3.4) for guidance on publication of photographs

A.3.4 Use of web-based publication tools

A.3.4a - Website (and other public facing communications)

Our school uses the public facing website www.muchbirchprimaryschool.co.uk for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

A.3.4b - Virtual Learning Environment (VLE) - Seesaw

Class teachers monitor the use of Seesaw by pupils regularly in all areas, but with particular regard to messaging and communication.

Staff use is monitored by the administrator.

User accounts and access rights can only be created by the school administrator and by LA administrators.

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to Seesaw.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the LP for the user may be suspended.

d) The user will need to discuss the issues with a member of SLT before reinstatement.

e) A pupil's parent/carer may be informed.

A visitor may be invited onto Seesaw by the administrator (usually the ICT coordinator) following a request from a member of staff.

A.3.5 Professional standards for staff communication

In all aspects of their work in our school teachers abide by the **Teachers' Standards** as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf. Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications. Staff will not befriend parents or pupils via social networking sites. As a member of staff you must not communicate or discuss school information via social networking sites.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

Teachers frequently discuss issues relating to password security and how it relates to staying safe in and out of school (see section C of this policy)

B.2.1 Filtering

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from Herefordshire ICT Services we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **online safety coordinator** (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Herefordshire school filtering service must:

- be logged in change control logs
- be reported to a second responsible person (the head teacher / ICT coordinator/online safety governor) within the time frame stated in section A.1.3 of this policy
- be authorised by a second responsible person prior to changes being made (this will normally happen anyway, as part of the process and will be the class teacher who originally made the request for the change).

All users have a responsibility to report immediately to class teachers / online safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

B.2.1c - Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's online safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- signing the AUP (a part of their induction process)
- briefing in staff meetings, training days, memos etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through online safety awareness sessions / newsletter etc

B.2.1d – Organisation of and changes to the filtering system

Two filtering policies, one for pupil internet access and a more relaxed one for staff access, are in used in our school. These policies apply to many primary schools.

Where a member of staff requires access to a website that is blocked under either policy, the process to unblock is as follows:

- The teacher makes the request to the school online safety coordinator, specifying which filtering policy needs altering.
- The online safety coordinator checks the website content to ensure that it is appropriate for use in this policy.
- If agreement is reached, the online safety coordinator contacts D and D services.

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment. Monitoring takes place as follows:

- Audit logs of internet activity are generated from time to time in schoolboy the online safety coordinator or requested of the Herefordshire ICT Schools Helpdesk

B.2.1f - Audit / reporting

Logs of filtering change controls and of filtering incidents are made available to

- the online safety governor within the timeframe stated in section A.1.3 of this policy
- the online safety committee (see A.1.1)
- the Herefordshire Safeguarding Children Board (HSCB) on request

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

B.2.2 Technical security

This is dealt with in detail in our schools **E-security Policy**. Please see that document for more information.

B.2.3 Personal data security (and transfer)

This is dealt with in detail in our schools **E-security Policy**. Please see that document for more information.

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see section C of this policy)

Section C. Education

C.1.1 Online safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of Computing, PSHCE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school – STAR programme Y6 with local PCOS
- We use the resources on CEOP's Think U Know site as a basis for our online safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)
- Learning opportunities for online safety are built into the Knowledge and Understanding sections of the Herefordshire Primary ICT Progression where appropriate and are used by teachers to inform teaching plans. (www.hereford-edu.org.uk/ict)
- Key online safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

C.1.2 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
    - Checking the likely validity of the URL (web address)
    - Cross checking references (can they find the same information on other sites)
    - Checking the pedigree of the compilers / owners of the website
    - See lesson 5 of the Cyber Café Think U Know materials below
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a basis for our online safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

C.1.2 Parent and carer awareness raising

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. 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. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Seesaw
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknowco.uk)

C.1.3 Wider school community understanding

The school may offer family learning courses in ICT, media literacy and online safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Glossary of terms

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 online 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 Netan be found.