Holy Redeemer Catholic Primary School

E-Safety Policy

(Policy and Procedure for the use of IT equipment in school)

Signed by:	
Head Teacher	Christina Hall
Chair of Governors	Alan Smith
Date Adopted	11.10.2017
Date of Review	12.10.2018

‘Through the Holy Redeemer we seek to grow in faith and love and become great people who make a difference in our world.’

Introduction

This Primary School E-Safety Policy Template is intended to help schools produce a suitable E-Safety policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies.

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its “Safeguarding Children in a Digital World” suggested:

> “That schools support parents in understanding the issues and risks associated with children’s use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too.”

The Byron Review “Safer Children in a Digital World” stressed the role of schools:

> “One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children’s workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area.”

Schools are expected, by Ofsted, to evaluate their level of e-safety (for example using the 360°Safe self review or similar tool) and e-safety is now subject to an increased level of scrutiny during school inspections. Many schools are opting to gain recognition for the quality of their ICT provision through ICTMark accreditation. The ICTMark Self Review Framework (SRF) contains a number of aspects regarding the school’s e-safety policies and provision.

Although e-safety is not mentioned explicitly in the new OFSTED Framework for School Inspection, January 2012, there is an increased emphasis on safeguarding. Several of the statements below can be directly related to aspects of e-safety:

Behaviour and safety of pupils at the school

When evaluating the behaviour and safety of pupils at the school, inspectors consider:

- pupils’ attitudes to learning and conduct in lessons and around the school
- pupils’ behaviour towards, and respect for, other young people and adults, including freedom from bullying and harassment that may include cyber-bullying and prejudice-based bullying related to special educational need, sexual orientation, sex, race, religion and belief, gender reassignment or disability
- how well teachers manage the behaviour and expectations of pupils to ensure that all pupils have an equal and fair chance to thrive and learn in an atmosphere of respect and dignity
- pupils’ ability to assess and manage risk appropriately and to keep themselves safe
- pupils’ attendance and punctuality at school and in lessons
- how well the school ensures the systematic and consistent management of behaviour.

Contents

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true 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
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- 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 or addictive 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 put in place to keep them safe) and so this policy also sets out how we educate children about 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 Worcestershire School Improvement team 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 E-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: the e-safety committee

Best practice is to appoint one of these. It is suggested that the committee is lead by the e-safety or safeguarding coordinator and is made up of representation from: children, senior leaders, staff, governors, etc. Once formed the group meets regularly (once a term) to review impact of the E-Safety Policy and to discuss ongoing e-safety issues in school. Where appropriate issues are referred on to other groups such as senior leadership teams, governors etc who may then decide to refer matters to the Worcestershire Safeguarding Children Board.

In small schools it may be felt that the functions of this group may be better delegated to other already existing groups, such as the School Council and still to refer issues as appropriate to other groups.

The school council regularly discusses issues relating to e-safety and when appropriate the staff representatives ask our school e-safety coordinator to attend its meetings. Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as the Worcestershire Safeguarding Children Board.

A.1.2 Responsibilities: e-safety coordinator

It is strongly recommended that each school should have a named member of staff with a day to day responsibility for e-safety; some schools may choose to combine this with the Child Protection Officer role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school and will very much depend on the size of the school.

Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety coordinator:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (*termly)*
- reviews weekly the output from monitoring software and initiates action where necessary
- meets regularly *(termly)* with the safeguarding governor to discuss current issues and review incident logs
- attends relevant meetings and committees of Governing Body

- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

A.1.3 Responsibilities: governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

- regular meetings with the E-Safety Co-ordinator (termly) with an agenda based on:
    - monitoring of e-safety incident logs
    - reporting to relevant Governors committee / meeting

A.1.4 Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator
- The head teacher and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with e-safety incidents (included in section 2.6 below) and other relevant Local Authority HR / disciplinary procedures)

A.1.5 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**.
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix 1)
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- they undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official school systems (see A.3.5)
- they embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme (see section C)

A.1.6 Responsibilities: ICT technician

Almost all Worcestershire primary schools employ the services of **IBS Schools,** who are aware of e-safety best practice, to manage their network and ICT systems. Schools employing other technical support should ensure that they are fully cognisant of the issues. It is reasonable to expect anyone providing technical support to assume responsibility **only** for the day-to-day maintenance of ICT systems. Ultimate responsibility for e-safety rests with the head teacher who must ensure that systems in school are fit for purpose. In practice this is usually collaboration between the technical support provider and educational experts in school and at the local authority.

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority E-Safety Policy and guidance)
- users may only access the school's networks through a properly enforced password protection policy as outlined in the school's e-security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

It is sometimes the case that a policy is written by one or two individuals within an institution and then shared with all stakeholders. This is not the right way to go about an e-safety policy. There are many issues that will be new to many people, which means that the more people involved in the writing of this policy the better its implementation will be. Some issues will be contentious and the debate that ensues in those areas will be valuable in developing understanding.

This e-safety policy has been developed (from a template provided by Worcestershire School Improvement Service) by a working group made up of:

- Head teacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors (especially the e-safety governor)
- Parents and Carers
- Pupils

Consultation with the whole school community has taken place through the following:

- *Staff meetings*
- *School Council*
- *INSET Day*
- *Governors meeting / subcommittee meeting*
- *Parents evening*
- *School website / newsletters*

Schedule for development / monitoring / review of this policy

This e-safety policy was approved by the governing body on:	*11/10/2017*
The implementation of this e-safety policy will be monitored by the:	*The e-safety coordinator*
Monitoring will take place at regular intervals:	*Annually*
The governing body will receive regular reports on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding:	*Annually*
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*10/10/2018*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Worcestershire Safeguarding Children Board e-safety representative Local Authority Designated Officer Worcestershire Senior Adviser for Safeguarding Children in Education West Mercia Police Diocesan representative

A.2.2 Policy Scope

This policy applies to **all members of the school community** (including teaching staff, wider workforce, 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 e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

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

A.2.3 Acceptable Use Agreements

These are short statements of which all members of the school community need to be aware and sign. They contain the basic points from this policy that are relevant to different groups in the school community. The school will need to decide how often these policies are signed (the policy statements in italics below suggest a starting point). The school will also need to check

the AUPs carefully to make sure that all are happy with the content. Induction policies need to reflect these statements.

These agreements can also be added to monitoring software so that users are reminded and must agree to them each time they log on to the network or access the internet, for example.

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers
- Community users of the school's ICT system

Acceptable Use Agreements are introduced at parents' induction meetings and signed by all children as they enter school (with parents possibly signing on behalf of children below Year 2) Children resign on entering KS2.

All employees of the school and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school's ICT system.

Induction policies for all members of the school community include this guidance.

A.2.4 Self Evaluation

Evaluation of e-safety is an ongoing 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.2.5 Whole School approach and links to other policies

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

Core ICT policies

ICT Policy	How ICT is used, managed, resourced and supported in our school.
E-Safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The e-safety policy constitutes a part of the ICT policy.
School systems and Data Security Policy	How we categorise, store and transfer sensitive and personal data and protect school systems. This links strongly and overlaps with the e-safety policy.
ICT Progressions	Four key documents and associated resources directly relating to learning covering the ICT Curriculum

Other policies relating to e-safety

Anti-bullying	How your school strives to eliminate bullying – link to cyber bullying
PSHE	E-Safety has links to staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. ***The e-safety policy forms a part of the school's safeguarding policy***
Behaviour	Positive strategies for encouraging e-safety and sanctions for disregarding it.
Use of images	**WCC guidance to support the safe and appropriate use of images in schools and settings**

A.2.6 Illegal or inappropriate activities and related sanctions

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. You will wish to review the list below to ensure that you agree and you may wish to add your own categories.

The sanctions tables will also need your attention to ensure that the ticks are in the right places for your policies (the ones offered are for guidance). Please be aware that there are obvious links here to other policies and you will need to ensure that they are all in line.

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 equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband 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 (e.g. 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
- Personal on-line shopping / commerce of an inappropriate nature
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

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 indicated on the following pages:

	Refer to:					Inform:	Action:		
Pupil sanctions *Schools should edit this table as appropriate to their institution.* *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Class teacher	E-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for action re filtering / security etc	Parents / carers	Remove of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔	✔	✔	✔	✔
Unauthorised use of non-educational sites during lessons	✔				✔				
Unauthorised use of mobile phone / digital camera / other handheld device	✔					✔	✔		
Unauthorised use of social networking / instant messaging / personal email	✔	✔			✔	✔		✔	
Unauthorised downloading or uploading of files	✔						✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔	✔		✔		✔	✔	
Attempting to access the school network, using another pupil's account	✔				✔		✔		
Attempting to access or accessing the school network, using the account of a member of staff	✔		✔		✔	✔		✔	
Corrupting or destroying the data of other users	✔		✔		✔	✔	✔	✔	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔	✔		✔	✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔			✔	✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔		✔					✔	
Using proxy sites or other means to subvert the school's filtering system	✔	✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔			✔	✔			
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔		✔

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✔		✔		✔		✔		

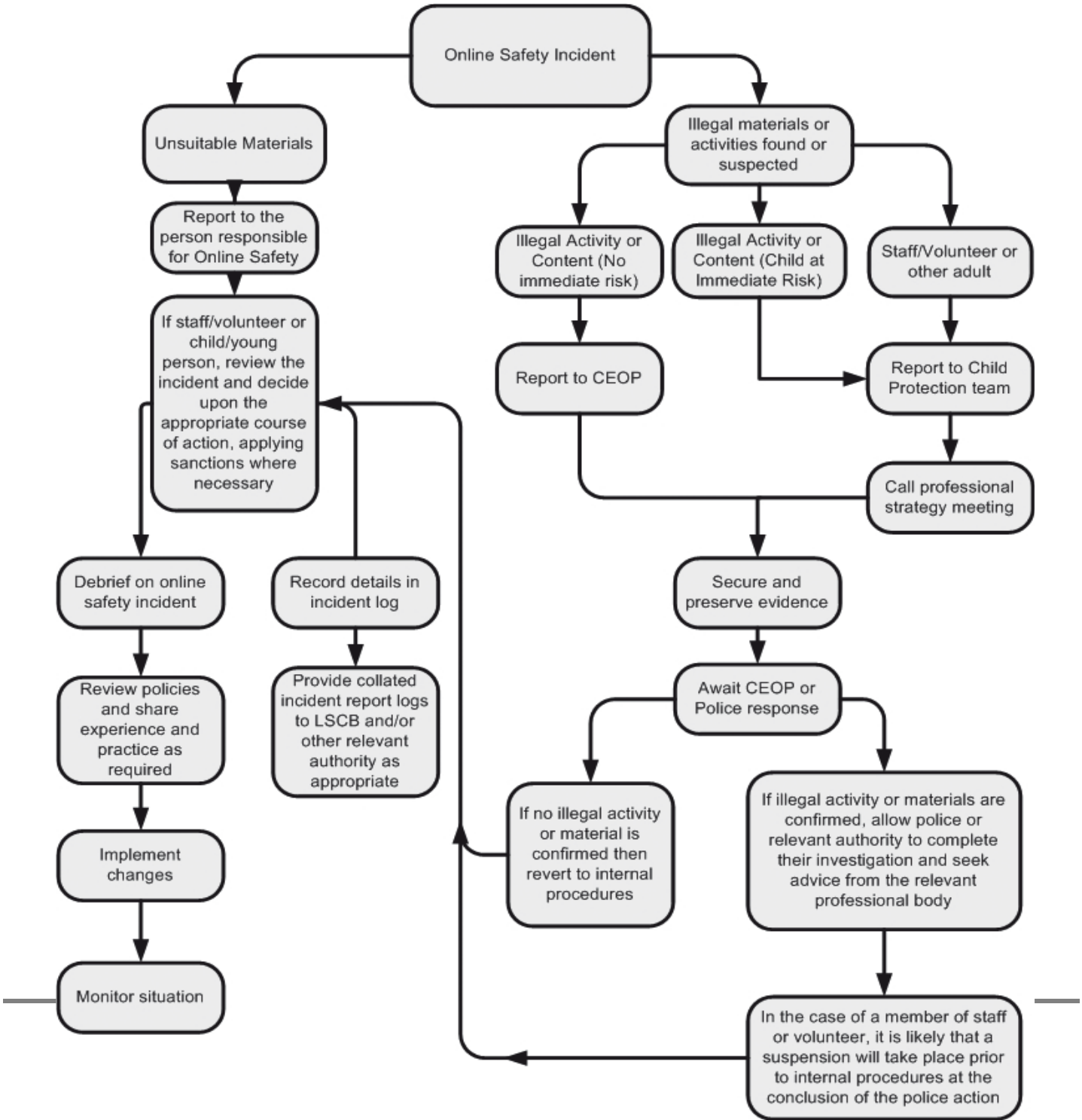
	Refer to:					Action:		
Staff sanctions *Schools should edit this table as appropriate to their institution.* *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Line manager	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✔	✔	✔	✔		✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔	✔				✔		
Unauthorised downloading or uploading of files	✔				✔	✔		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔	✔			✔	✔	✔	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✔	✔	✔		✔	✔		✔
Deliberate actions to breach data protection or network security rules	✔	✔	✔		✔	✔	✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔				✔	✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔				✔	✔	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✔	✔			✔			
Actions which could compromise the staff member's professional standing	✔	✔						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔					✔		
Using proxy sites or other means to subvert the school's filtering system	✔				✔	✔		✔
Accidentally accessing offensive or pornographic	✔	✔			✔	✔		

material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔	✔
Breaching copyright or licensing regulations	✔					✔		
Continued infringements of the above, following previous warnings or sanctions	✔	✔			✔			✔

A.2.7 Reporting of e-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



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

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies. E.g. few schools currently allow pupils to use mobile phones in lessons, while a small number recognise their educational potential and allow their use. This section may also be influenced by the age of the pupils. The list below reflects the current policy for the majority of Worcestershire primary schools; you may wish to add some policy statements of your own (in and out of the table) as well as modify the response to those already there.

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
  - ✓ Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
  - ✓ Members of staff are free to use these devices outside teaching/working time.
  - ✓ A school mobile phone is available for all professional use (for example when engaging in off-site activities) and members of staff should not use their personal device for school purposes except in an emergency.
- Pupils are not currently permitted to bring their personal hand held devices into school except in exceptional circumstances and by agreement with the head teacher.

	Staff / adults				Pupils			
Personal hand held technology *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	✔					✔		
Use of mobile phones in lessons (teachers, pupils and support staff)/during work hours (cleaners)				✔				✔
Use of mobile phones in social time		✔						✔
Taking photos, videos or voice recordings on personal phones or other camera devices				✔				✔
Use of hand held devices e.g. PDAs, gaming consoles		✔					✔	

A.3.2 Use of communication technologies

The range of communication technologies is growing rapidly and such tools are widely used by all outside school. Many schools now provide access to such tools through a learning platform or virtual learning environment. These tools are easily monitored and therefore safer than most used outside school. Educational blogs and chat rooms are provided outside these tools and professionals in school will need to make decisions on an ongoing basis as to which are appropriate for use in school. The statements and tables below reflect the current policy for the

majority of Worcestershire primary schools; you may wish to add some policy statements of your own (in and out of the table) as well as modify the response to those already there.

A.3.2a - Email

Access to email is provided for all users in school via the Worcestershire Learning Gateway using their Global IDs.

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 (e.g. 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 program 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 may only access personal email accounts on school systems for emergency or extraordinary purposes (if they are not blocked by filtering)
- Users must immediately report to their class teacher / e-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 they must not respond to any such email.

	Staff / adults				Pupils			
Use of Email *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of personal email accounts in school / on school network		✔						✔
Use of school email for personal emails		✔						✔

A.3.2b - Social networking (including chat, instant messaging, blogging etc)

	Staff / adults				Pupils			
Use of social networking tools *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain	Allowed for selected	Not allowed	Allowed	Allowed at certain	Allowed with staff	Not allowed
Use of non educational chat rooms etc				✔				✔
Use of non educational instant messaging				✔				✔
Use of non educational social networking sites				✔				✔

Use of non educational blogs				✔				✔

A.3.2c - Videoconferencing

Videoconferencing technology is available to schools via a number of routes and many schools are beginning to make good educational use of these. The kinds of technology include:

- Live video through the WCC provided Communicator and Live Meeting services.Communication tools that allow audio and video communication across the internet via a variety of providers using an inexpensive webcam (appropriate only for individuals or small groups of children where quality is less crucial)
- More expensive dedicated systems providing high quality whole class conferencing accessing connections through the National Education Network

Desktop video conferencing and messaging systems linked to WCC Broadband via MS Communicator is the preferred communication option in order to secure a quality of service that meets school curriculum standards.

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

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

Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.

Videoconferencing is normally supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the class teacher before making or answering a videoconference call.

Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in school (see section A.2.3 and Appendix 1). Only where permission 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.

A.3.3 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will need to inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm. Schools should refer to the WCC guidance document on the safe and appropriate use of images in settings (Dec 2011)

- 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

Different rules need to apply for public facing communication (e.g. the school website) and that which is accessible only to members of the school community (e.g. a learning platform)

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

Our school uses the public facing website (*holyredeemerschoolpershore.org)* only 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 will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Pupil's names will be used on the website with parents' permission, and only then when necessary.
- Detailed calendars will not be 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, without parents' permission
  - ✓ where possible, photographs will not allow individuals to be recognised
  - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

A.3.4b – Learning Platform

A learning platform can offer a wide range of benefits to teachers, pupils and parents as well as supporting school management and administration. It can enable pupils and teachers to collaborate in and between schools, can be used to share resources and tools for a range of topics, create and manage digital content, and for pupils to develop online and secure e--portfolios of work.

Any learning platform must be used subject to careful monitoring by Senior Leadership Team (SLT). As the usage grows throughout the school more issues could arise regarding content, inappropriate use and online behaviour by users.

Class teachers monitor the use of the learning platform by pupils regularly during all supervised sessions, but with particular regard to messaging and communication.

Staff use is monitored by the super-user/administrator.

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

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 the learning platform.

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 learning platform may be suspended for the user.

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 the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

A.3.5 Professional standards for staff communication

Teachers are governed by clear professional standards. The government has recently announced that it intends to replace those devised and published by the TDA with new ones. Although the replacement standards contain no specific references to ICT there are particular codes of conduct that relate to e-safety, as well as more generally. It is a school's responsibility to act in the best interests of the children it serves, and that is what this section of the policy is about. The policy statements also need to ensure that the professionalism of teachers is preserved and that the integrity is not compromised.

In all aspects of their work in our school, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA (current until the end of August 2012):

http://www.tda.gov.uk/teacher/developing-career/professional-standards-guidance/~/media/resources/teacher/professional-standards/standards_a4.pdf

These will be superseded by the **Teachers' Standards** as described by the DfE effective from September 2012: 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, learning platform 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 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

This is dealt with in detail in our school's ***E-security Policy***. Please refer to that document for more information.

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy)

B.2.1 Filtering

Worcestershire schools automatically receive internet filtering via the broadband network. This service is intended to prevent users accessing material that would be regarded as illegal and / or inappropriate in an educational environment. Because the content on the web changes dynamically and new technologies are constantly being developed, it is not possible for any filtering service to be 100% effective. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

The current Worcestershire filtering service provides flexibility for schools to decide on their own levels of filtering security. It is possible to add to or override some of the sites filtered centrally. This functionality can be switched on for individual schools where it is requested providing certain requirements have been met and the school can demonstrate that it is aware of the implications and processes involved. Schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

As the use of the internet becomes more widespread and access becomes available through a wider range of technologies, users become more sophisticated in their internet use, therefore schools need continually to review their filtering and monitoring policies.

Schools will however need to consider carefully the issues raised and modify the statements below in the light of decisions made on:

- Whether they will adopt the Worcestershire filtering without change
- Whether to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users.
- Where responsibility lies for such decisions, and how checks and balances are put in place.
- What other system, including user monitoring systems, (if any) will be used to supplement the filtering system and how these will be used.

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 Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

It is recognised that the school can take full responsibility for filtering on site but current requirements do not make this something that we intend to pursue at this moment.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **e-safety coordinator** (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering in line with this policy 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 Worcestershire school filtering service must (schools should choose relevant response(s):

- be logged in change-control logs after discussion with the head teacher

All users have a responsibility to report immediately to class teachers / e-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 have been filtered.

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 e-safety education programme (see section C of this policy).

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

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the school e-safety coordinator.
- The e-safety coordinator checks the website content to ensure that it is appropriate for use in school.

THEN (if the school is not controlling its own filtering)

- If agreement is reached, the e-safety coordinator makes a request to the Broadband Team
- The Broadband helpdesk will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites in advance of teaching sessions.
- School Improvement Service Learning Technologies staff may then be notified of websites that have been unblocked to review them in partnership with the Broadband Team. If sites are found to not be appropriate, access will be discussed with the school and then removed.

B.2.1e - Monitoring

All schools are expected to supplement their filtering systems with additional monitoring systems. Schools should include such information in this section, including – if they wish – details of systems that are in use. Most Worcestershire primary schools subscribe to Policy Central from Forensic Software. They have access to a remote console through which they should review all desktop or keystroke captures regularly (weekly is recommended to prevent this becoming a lengthy activity).

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 as indicated in the. Monitoring takes place as follows:

- Identified member(s) of staff reviews the Policy Central console captures weekly
- "False positives" are identified and deleted.
- Potential issues are referred to an appropriate person depending on the nature of the capture.

- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

B.2.1f - Audit / reporting

Filter change-control logs and incident logs are made available to:

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

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

For example, the evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary.

B.2.2 Technical security

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document for more information.

B.2.3 Personal data security (and transfer)

This is dealt with in detail in **IBS School's System and Data Security advice**. 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 E-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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-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.

E-Safety education will be provided in the following ways:

statements will need to be adapted, depending on the age of the students / pupils and the school's structure

- A planned e-safety programme is provided as part of ICT, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school
- We use the resources on the Worcestershire E-safety website as a source of e-safety education resources http://www.wes.networcs.net (e.g. Hector's World at KS1 and Cyber Café and SAFE social networking at KS2)
- Learning opportunities for e-safety are built into the *Knowledge and Understanding* sections of the *Worcestershire Primary ICT Progressions* where appropriate and are used by teachers to inform teaching plans.

- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement (see Appendix 1) 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, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging children to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

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
  - ✓ Referring to other (including non-digital) sources
- Pupils will 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 e-safety education* *http://www.thinkuknow.co.uk/teachers/resources/*

C.1.3 The contribution of the children to e-learning strategy

It is our general school policy to encourage children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy (see section A.1.1)

C.2 Staff training

It is essential that all staff – including non-teaching staff - receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- *It is expected that some staff will identify e-safety as a training need within the performance management process.*

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-safety Co-ordinator will be CEOP trained.
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, the WSCB and others.
- All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from Worcestershire School Improvement Learning Technologies Team when appropriate

C.3 Governor training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or School Improvement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The e-safety governor works closely with the e-safety coordinator and reports back to the full governing body (see section A.1.3)

C.4 Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-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,
- Parents evenings
- Reference to the parents materials on the Worcestershire E-safety website (http://www.wes.networcs.net) or others (see Appendix 4)

C.5 Wider school community understanding

The school may offer family learning courses in ICT, media literacy and e-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. 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.

Community Users who access school ICT systems / website / learning platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Agreement (see Appendix 1) before being provided with access to school systems.

Appendix 1 – Acceptable Use Agreement templates

Sections in the following AUAs that include advice or guidance are written in a box like this in small print. It is anticipated that schools will remove these sections from their final AUA document. Schools should review and amend the contents of this AUA to ensure that it is consistent with their E-Safety Policy and other relevant school policies. Due to the number of optional statements and the advice / guidance sections included in this template, it is anticipated that the final AUA will be more concise.

It is suggested that when the Pupil AUA is written that a copy should be attached to the Parents / Carers AUA to provide information for parents and carers about the rules and behaviours that pupils have committed to by signing the form.

Appendix 1a – Acceptable use policy agreement – pupil (KS1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

(The school will need to decide on the age at which they would expect children to sign the agreement - for younger children the signature of a parent / carer should be sufficient)

I understand these computer rules and will do my best to keep them

My name:	
Signed (child):	
OR Parent's signature:	
Date:	

Appendix 1b – Acceptable use policy agreement – pupil (KS2)

I understand that while I am a member of Holy Redeemer Catholic Primary School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows

KS2 Pupil Acceptable Use Agreement Form

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Appendix 1c - Acceptable Use Agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the e-safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the e-safety policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the e-safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the e-safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency (A.3.2).

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up in accordance with relevant school policies (see **IBS Schools Systems and Data Security advice**).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (see e-security policy). Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and to my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police (see section A.2.6).

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	

Date:	

Appendix 1d - Acceptable use policy agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- young people will be responsible users and stay safe while using ICT (especially the internet).
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Child's name	
Parent's name	
Parent's signature:	
Date:	

Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe and responsible use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Parent's signature:	

Date:	

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use the school's digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. The school will also ensure that when images are published, the young people cannot be identified by name.

As the parent / carer of the above pupil, I agree to the school taking and using digital images of my child(ren). I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events which include images of children, I will abide by these guidelines in my use of these images.

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website and in the school's learning platform.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

Permission to for my child to participate in video-conferencing

Videoconferencing technology is used by the school in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas partner school. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

The school's e-safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Appendix 1e - Acceptable use policy agreement – community user

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

I will be responsible in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials described above.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community user Name:	
Signed:	
Date:	

Appendix 2 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Sample documents for recording the review of and action arriving from the review of potentially harmful websites can be found in the PDF version of the SWGfL template e-safety policy (pages 36-38): http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

Appendix 3 – Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

B. CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- **The site promotes equal and just representations of racial, gender, and religious issues.**
- **The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.**
- **The site does not link to other sites which may be harmful / unsuitable for the pupils**
- The content of the website is current.

C. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 4 - Supporting resources and links

The following links may help those who are developing or reviewing a school e-safety policy.

General

South West Grid for Learning "SWGfL Safe" - http://www.swgfl.org.uk/Staying-Safe

Child Exploitation and Online Protection Centre (CEOP) http://www.ceop.gov.uk/

ThinkUKnow http://www.thinkuknow.co.uk/

ChildNet http://www.childnet-int.org/

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

Byron Reviews ("Safer Children in a Digital World") - http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews

Becta – various useful resources now archived http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk

London Grid for Learning - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety

Kent NGfL http://www.kented.org.uk/ngfl/ict/safety.htm

Northern Grid - http://www.northerngrid.org/index.php/resources/e-safety

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

WMNet – http://www.wmnet.org.uk

WES Worcestershire E-Safety Site – http://www.wes.networcs.net

EU kids Online http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Cyber Bullying

Teachernet "Safe to Learn – embedding anti-bullying work in schools" (Archived resources)

http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

East Sussex Council - Cyberbullying - A Guide for Schools:

https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Social networking

Digizen – "Young People and Social Networking Services": http://www.digizen.org.uk/socialnetworking/

Ofcom Report: Engaging with Social Networking sites (Executive Summary)

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

Connect Safely - Smart socialising: http://www.blogsafety.com

Mobile technologies

"How mobile phones help learning in secondary schools":

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

"Guidelines on misuse of camera and video phones in schools"
http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

See also Becta (archived) resources above

Parents' guide to new technologies and social networking

http://www.iab.ie/

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website: http://www.swgfl.org.uk/staying-safe

BBC Webwise: http://www.bbc.co.uk/webwise/

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

NCH - http://www.stoptextbully.com/

Chatdanger - http://www.chatdanger.com/

Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

London Grid for Learning: http://www.lgfl.net/esafety/Pages/safeguarding.aspx?click-source=nav-toplevel

Appendix 5 - Glossary of terms

AUA	Acceptable Use Agreement – 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 archived and still relevant)
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
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE for DfE
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 Regional Broadband Consortia
KS1; KS2	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
Learning platform	An online system designed to support teaching and learning in an educational setting
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 – a web address
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)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)