GUIDANCE ON THE DEVELOPMENT OF AN E-SAFETY POLICY FOR VOLUNTARY AIDED CATHOLIC SCHOOLS

July 2010

DIOCESAN SCHOOLS COMMISSION

Serving Catholic Schools in the Archdiocese of Birmingham

Archdiocese of Birmingham Registered Charity No 234216

ARCHDIOCESE OF BIRMINGHAM

DIOCESAN SCHOOLS COMMISSION

GUIDANCE ON THE DEVELOPMENT OF AN E-SAFETY POLICY FOR VOLUNTARY AIDED CATHOLIC SCHOOLS

1 INTRODUCTION

1.1 Significant changes and developments in recent years have occurred in all areas of the curriculum and none more so than in information and communication technology (ICT) and these continue at an ever-increasing pace.

1.2 Whilst recognising that the use of ICT in school is of great benefit to pupils, the Diocesan Schools Commission (DSC) supports the view that the school must address e-Safety issues and plan accordingly to ensure appropriate, effective and safe use of electronic communications.

1.3 Governors and senior leaders should be aware that this guidance does not constitute an e-Safety Policy. The e-Safety Policy should be drafted by the headteacher and staff using any relevant local authority (LA) guidance and be approved by the governors. The school should consult parents and carers and young people and the policy should then be shared with all parties, implemented fully and undergo an annual review.

1.4 An e-Safety policy will need to address a number of technical, educational and management issues and the school may feel that it does not have the expertise to write its own policy.

1.5 The LA may be able to supply the school with a policy template, providing material to stimulate debate amongst staff and a structure for policy writing.

1.6 If local help is not available, the school may wish to visit www.clusterweb.org.uk or www.kenttrustweb.org.uk?e-safety for the latest advice and a Kent County Council template. Any school is free to use and adapt the Kent County Council materials as they wish but those outside Kent are asked to e-mail safety@kent.gov.uk and acknowledge the copyright.

1.7 The school should also consider government guidance in areas such as e-mail, social networking and publishing.

1.8 This guidance has been developed from documents produced by Kent County Council's Children, Families and Education Directorate, who have given permission for their materials to be copied and adapted. Other

material by kind permission of Oxfordshire County Council, Education Walsall and Warwickshire County Council.

2 RATIONALE

2.1 To maintain its distinctiveness the Catholic school 'must be able to speak for itself, effectively and convincingly' and place the person of Christ and the teachings of the Catholic Church at the centre of every aspect of school life.

2.2 Governors, the headteacher, staff, parents and pupils must continue to support the primary purpose of Catholic education and play their full part in the life of the school, whilst engaging positively with the changes and developments in education today and in the future. The Gospel of life and the dignity of the human person it promotes should be experienced in the care, support and guidance given by the school to its pupils.

2.3 The dangers and risks associated with the increasing use of ICT in school, demand an informed and skilled staff supported by governors and parents, to ensure pupil safety at all times.

2.4 Furthermore it is not acceptable for a Catholic school to be compromised by staff who are complacent or negligent about adhering to e-Safety rules.

2.5 This guidance will alert the school of the need to:

- explore any issues in the context of the ethos of a Catholic school;
- develop a policy that will enhance the protection of pupils, staff, governors and others using the school's systems;
- educate children and young people about the benefits, risks and responsibilities of using ICT and provide safeguards to enable users to control their online experiences;
- raise awareness of the responsibilities of the governing body, staff, pupils and parents;
- engage with and use local authority support and technical services as necessary;
- establish an annual review process and update the e-Safety Policy as necessary.

3 WHAT IS E-SAFETY?

3.1 E-Safety is a child safety issue not an ICT one and an effective policy should form part of the school's 'duty of care' which ensures the protection of all children. A new national e-Safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP) and detailed materials are available from www.ceop.gov.uk.

3.2 It is widely accepted that pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities.

3.3 The World Wide Web, e-mail, blogs and social networking sites all transmit information using the Internet's communication infrastructure at low cost. Anyone with access to a computer can send messages, discuss ideas and publish material with little restriction.

3.4 These features of the Internet make it an invaluable resource used by millions of people every day and the exchange of ideas, social interaction and learning opportunities on offer, are greatly beneficial.

3.5 The new technologies also bring opportunities for staff to be more creative and productive in their work.

3.6 However, the Internet is an unmanaged, open communications channel and much of the material on the Internet is published for an adult audience which can be unsuitable for pupils and can place them in embarrassing, inappropriate and even dangerous situations.

3.7 All users should have an entitlement to safe internet access at all times and should be aware that photographs, videos and information can be easily modified to cause harm.

3.8 The school must decide on the right balance between controlling access, setting boundaries, clarifying rules and educating students in responsible use.

3.9 Staff and pupils must also learn that publishing personal information could compromise their security and that of others, and this information once 'posted' is nearly impossible to remove.

3.10 It must be made clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is 'unauthorised'. However, the school should be aware that a disclaimer is not sufficient to protect it from legal challenge or a claim of personal injury. Therefore the school needs to provide evidence that it has taken reasonable action to protect users, it has put in place measures to monitor usage and that policy is turned into practice.

3.11 The school's policy must also clearly state that the school reserves the right to monitor e-mail and website use. It should be made clear that such monitoring is for the protection of the school community and that all information will be treated in the strictest confidence.

3.12 As employers in a VA school, governors must be mindful of their duty of care towards the staff. Governors must be satisfied that all staff understand the risks involved, are able to protect themselves and have the ability and confidence to react adequately to any issues that may be raised by young people.

4 RESPONSIBILITIES OF SCHOOL STAFF

4.1 The school will try to ensure that staff and volunteers have good access to ICT to enhance the learning opportunities for students/pupils, and in return expect staff and volunteers to agree to be responsible users.

4.2 An example of an Acceptable Use Policy Agreement is set out in **Appendix 1.**

4.3 This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies, for educational, personal and recreational use;
- that school ICT systems and users are protected from accidental or deliberate misuse, that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of ICT in their everyday work;

4.4 As ICT is developing rapidly, many members of staff may not be fully aware of the on-line risks and how to teach e-Safety adequately. Staff may also be unsure of how to discuss e-Safety issues with pupils. Therefore advice and training should be obtained from LA advisers, e-Safety officers, or child protection officers.

4.5 E-Safety depends on the staff, governors, parents and where appropriate, the pupils themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples.

4.6 It is strongly recommended that all staff should sign an information systems code of conduct on appointment and accept that the school can monitor network and Internet use.

4.7 Many LAs encourage the school to appoint an e-Safety Co-ordinator. This could be the Designated Child Protection Co-ordinator, a member of the SLT, the ICT Co-ordinator or a subject teacher.

4.8 The e-Safety Co-ordinator should receive support and advice from the LA e-Safety Officer, the appropriate child protection support services and where necessary, the police.

4.9 The e-Safety Co-ordinator should maintain the e-Safety Policy, manage e-Safety training, co-ordinate risk assessments and keep abreast of local and national e-Safety awareness campaigns.

4.10 Apart from seriously compromising the trust between teachers and pupils, a member of staff who uses e-mail or the Internet for inappropriate reasons is in breach of their contract and risks dismissal. This could also apply to someone who flouts security advice.

4.11 Staff in a Catholic school must also be mindful that they would contravene their contract of employment by acting in any way that could be 'detrimental or prejudicial' to the Catholic character of the school.

4.12 Staff that manage filtering systems or monitor ICT use must be appropriately supervised and procedures must define how inappropriate or illegal ICT use is to be reported to senior management.

4.13 Any allegation of inappropriate behaviour must be reported to senior management and investigated with great care and sensitivity.

4.14 Staff must be made aware of the potential dangers to themselves and take sensible precautions when monitoring ICT use, for instance when viewing inappropriate images to investigate their source.

4.15 It should be noted that nationally, the Child Exploitation and Online Protection Centre (CEOP) has been set up by the Home Office to safeguard children's online experiences and track down and prosecute offenders.

5 CYBER BULLYING

5.1 Cyber Bullying is the use of information and Communications Technology, particularly mobile phones and the internet, deliberately to upset someone else. It can affect staff as well as pupils. Schools should state in their anti-bullying and behaviour policies how they will address cyber bullying, including the bullying of staff. Those affected should know who in the school they should go to for assistance.

5.2 Staff must take care of their passwords, use firewalls and anti-virus software and should withhold their own number if they need to phone students homes or mobiles. They should not respond to malicious texts or e-mails but they should save evidence and report incidents.

6 E-SAFETY FOR PRIMARY PUPILS

6.1 The school has a duty to provide students with safe and secure Internet access as part of their learning experience.

6.2 Most Internet use in primary schools is safe, purposeful and beneficial to learners but there is always an element of risk. For the youngest pupils, the greatest risk is through inadvertent access. Even an innocent search can occasionally turn up links to adult content or violent imagery.

6.3 Fast broadband means that inappropriate images can appear almost instantaneously and children can unwittingly follow a series of links to undesirable content. A procedure should be agreed with all staff on what to do, and how to handle the situation with pupils. This could include closing or minimising the image or window immediately, talking to pupils about what has happened, reassuring them and later, investigating the history of visited sites and how the pupils accessed them.

6.4 In view of the risks, primary pupils should be supervised at all times when using the Internet. However, many teachers feel that there is a far greater problem for pupils in the amount of irrelevant or incomprehensible material typically yielded by Internet searches.

6.5 For these reasons some LAs may not allow primary pupils to use Internet-wide search engines such as 'Google', and all teachers should think very carefully before doing so. If 'Google' is to be used, the school must make sure that strict filtering is applied.

6.6 However, the school should realise that no filter-based search engine is completely safe, as even with strict filtering, unsuitable content can be readily found when using a modern network.

6.7 For external e-mail, there is no need for pupils to use individual accounts. A class e-mail address may be set up, and moderated by the teacher. For examples and further advice contact the LA advisers.

7 E-SAFETY FOR SECONDARY PUPILS

7.1 Many of the issues for primary aged pupils are also relevant to secondary pupils but there are further considerations.

7.2 The school's Internet access should be designed expressly for student use and it will include filtering appropriate to the age of the student. Senior staff should take responsibility for regularly checking that filtering and monitoring is suitable, effective and reasonable.

7.3 However, due to the international scale and connected nature of the Internet, it is impossible to guarantee that unsuitable material will never appear on a school computer.

7.4 Students need to be taught what is and what is not acceptable and given clear objectives for Internet use.

7.5 Fair rules, devised by the students, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions for internet use.

7.6 The balance between educating pupils to take a responsible approach and the use of regulation must be judged carefully. The unsupervised use of 'chat rooms' for example present immediate dangers.

7.7 The school should keep an up-to-date record of access levels granted to all network users and take all reasonable precautions to ensure that users access only appropriate material. However, it is important that technical staff do not take on themselves the responsibility for educational or disciplinary issues.

7.8 Parents should be informed that students will be provided with supervised Internet access. Parents and students should sign an acceptable use agreement and understand that the e-Safety Policy will work in

conjunction with other policies including the Behaviour Policy, Anti-Bullying Policy and Curriculum Policy.

7.9 Pupils also need to know how to cope if they come across inappropriate material in other locations such as youth clubs, libraries, public access points and their homes.

8 E-SAFETY FOR PUPILS WITH ADDITIONAL NEEDS

8.1 Pupils need to learn safety rules in a way that does not frighten them, which gives them confidence to know what to do in certain situations and how to avoid certain 'risks'.

8.2 However, the most ICT capable children may be the most vulnerable and it is often those who have poor social skills that are more at risk from inappropriate online contact.

8.3 It would seem to be relevant therefore for the school to consider its e-Safety Policy in relation to this specific group of pupils.

8.4 For advice on strategies regarding teaching e-Safety to pupils with additional needs, please refer to LA guidance. Alternatively, guidance can be found at www.kenttrustweb.org.uk?e-safety.

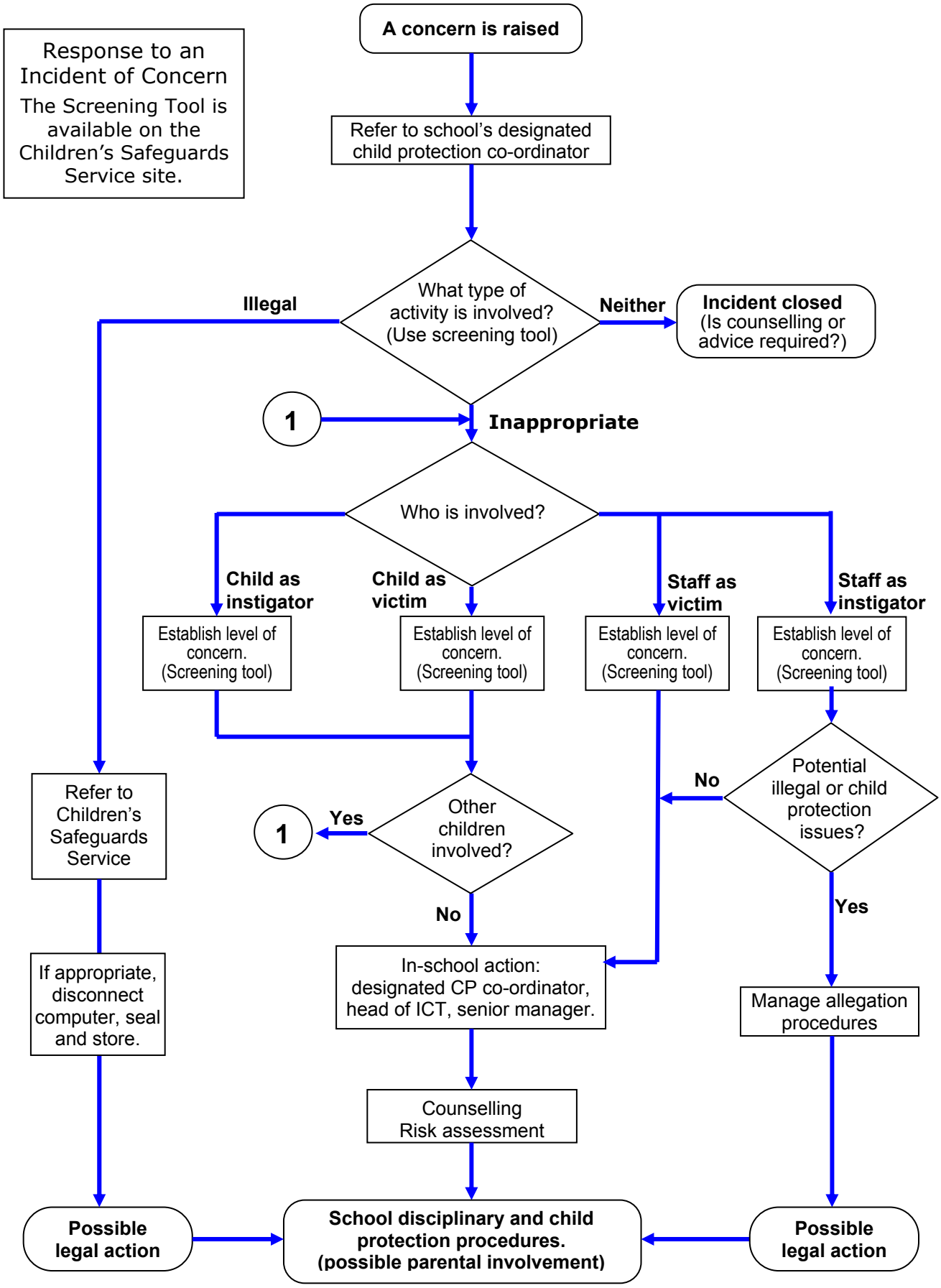
9 RESPONSE TO AN INCIDENT OF CONCERN

9.1 A school's e-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using ICT. They need to behave responsibly, with respect for others while keeping safe and secure from people acting inappropriately or even illegally.

9.2 Teachers' observation of behaviour is essential in detecting danger to pupils. Reported incidents will vary from a prank or thoughtless action to considered illegal activity.

9.3 It is important that staff determine what action they can take and when to report an incident of concern to the school's Designated Child Protection Co-ordinator or the e-Safety Co-ordinator. Matters can then be handed over to the LA Child Protection Officer or the Police if that becomes necessary.

9.4 The flowchart on the next page is the work of Child Protection Officers and the Kent CC e-Safety Officer and illustrates an approach to investigating an incident of concern. Information on its use can be found at Kent County Council Children's Safeguards Service: www.clusterweb.org.uk?safeguards.


Response to an Incident of Concern
The Screening Tool is available on the Children's Safeguards Service site.
A concern is raised
Refer to school's designated child protection co-ordinator
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
1
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Refer to Children's Safeguards Service
1
Yes
Other children involved?
No
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action

This guidance has been agreed between representatives of the Catholic Archdiocese of Birmingham Schools Commission and the teacher organisations listed below:

The Association of Teachers and Lecturers

The National Association of Headteachers

The National Association of Schoolmasters Union of Women Teachers

The National Union of Teachers

The Association of School and College Leaders

The guidance was adapted from the Kent County Council Children, Families and Education Directorate 'Schools e-Safety Policy Guidance 2007' edited by Peter Banbury

The Diocesan Schools Commission would like to thank Kent County Council, Oxfordshire County Council, SERCO/Education Walsall and Warwickshire County Council for the use of their materials.

13 May 2010.

APPENDIX 1

SAMPLE ACCEPTABLE USE POLICY AGREEMENT

1 INTRODUCTION

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 recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. 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.

2 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 (eg laptops, email, VLE etc) out of school. (schools should amend this section in the light of their policies which relate to the use of school systems and equipment 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems);
- 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, I become aware of, to the appropriate person.

3 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 / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured;

- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites);

- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications);

- I will not engage in any on-line activity that may compromise my professional responsibilities.

4 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:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (schools should amend this section in the light of their policies which relate to the use of staff devices);

- I will not use personal email addresses on the school ICT systems. (schools should amend this section in the light of their email policy – some schools will choose to allow the use of staff personal email addresses in 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 ensure that my data is regularly backed up, in accordance with relevant school policies;

- 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. (schools should amend this section in the light of their policies on installing programmes / altering settings);

- 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 (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted;

- I understand that data protection policy requires that any staff or student / 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.

5 WHEN USING THE INTERNET IN MY PROFESSIONAL CAPACITY OR FOR SCHOOL 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);

6 I UNDERSTAND THAT I AM RESPONSIBLE FOR MY ACTIONS IN AND OUT OF SCHOOL:

- I understand that this Acceptable Use Policy 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 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 Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Example from SERCO/Education Walsall

APPENDIX 2

ORGANISATIONS OFFERING e-SAFETY GUIDANCE

The first point of contact should be the local authority e-Safety Officer, however a number of useful web-sites and addresses are included here**.**

(N.B. some web-sites have content from the U.S.A. or Australia.)

GENERAL GUIDANCE

BBC Chat Guide for teachers 8 – 11 and 11 – 16 guides are available for download
http://www.bbc.co.uk/chatguide/teachers/index.shtml

Becta
http://www.becta.org.uk/schools/esafety

CFE e-Safety Officer, KCC Children Families & Education
e-mail: safety@kent.gov.uk Tel: 01622 696590

Childnet – Know it All
http://www.childnet-int.org/kia

e-Safety in Schools
http://www.kenttrustweb.org.uk?esafety

GetNetWise – This website has a series of video clips explaining issues regarding internet safety.
http://www.getnetwise.org/

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Proficiency Scheme
http://www.gridclub.com/teachers/t_internet_safety.html

Internet Safety for Schools Information on filtering software, Acceptable User Policies etc. **(Australian based - contains advertisements on opening page)** http://teacher.scholastic.com/professional/teachtech/internetsafety.htm

Internet Safety Zone (Contains advertising links to 'partner companies' on opening page)
http://www.internetsafetyzone.com/

Intuitive media – Pepper and Poppy, Grid Club, Gold Star Café
http://www.intuitivemedia.com/

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

Teachernet – use of photographs and videos in school
http://www.teachernet.gov.uk/wholeschool/familyandcommunity/childprotection/usefulinformation/photoschoolevent/

The Teacher's Guide Internet Safety Guide leaflet with information for parents. **(U.S. content)**
http://www.theteachersguide.com/Internetsafety.html

Think U Know website (Home Office leaflet on keeping children safe when using Internet)
http://www.thinkuknow.co.uk/

CHILD PROTECTION

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Childline
http://www.childline.org.uk/

Children's Safeguards Service
www.clusterweb.org.uk?safeguards

Internet Watch Foundation (This is for reporting illegal content)
http://www.iwf.org.uk/

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Virtual Global Taskforce – For reporting abuse (Always follow the school's procedures)
http://www.virtualglobaltaskforce.com/

Becta has also produced three booklets that are essential reading:

- Safeguarding children in a digital world Ref: BEC1-15401;
- E-safety (revised) Ref: BEC1-15402;
- Signposts to safety, Key Stage 3 + 4, Ref: BEC1-15274.

INTERNET SAFETY – WEB-SITES FOR PUPILS

CBBC
http://www.bbc.co.uk/cbbc/help/safesurfing/index.shtml

4Kids Safe Surf
http://www.4kids.org/safesurf/

Internet Super Heroes
http://www.internetsuperheroes.org/

NetSmartz Teens (U.S. content)
http://www.netsmartz.org/netteens.htm

Websafe Crackerz
http://www.websafecrackerz.com/

INTERNET SAFETY – WEB-SITES FOR PARENTS

Bullying Online
http://www.bullying.co.uk/

Chat Danger
http://www.chatdanger.com/

Childnet International Parents' Support -
http://www.childnet-int.org/safety/parents.aspx

The DCSF Parent Centre
http://www.parentscentre.gov.uk/usingcomputersandtheinternet/

Supplied by Kent County Council and Oxfordshire County Council

APPENDIX 3

AN EXAMPLE OF AN E-LEARNING CODE OF CONDUCT

This code of conduct applies at all times, in and out of school hours, whilst using school equipment.

Internet, e-mail and access to a learning platform will be provided for you to conduct research, communicate with others and access your personal on-line storage space as well as learning resources but only on the understanding that you agree to follow this code. This code of conduct is not intended to be exhaustive. At all times you should use e-learning resources in an appropriate and responsible manner.

You should:

- ✓ Only access sites which are appropriate for use in school. *This also applies outside lesson time*
- ✓ Be aware that your actions on the Internet, when using e-mail and in the learning platform can be seen and monitored
- ✓ Be aware that information on an Internet web site may be inaccurate or biased. Try to verify the information using other sources, if possible, before using it
- ✓ Be careful of what you say to others and how you say it. Never give *your name, home address, telephone numbers or any personal information about yourself or others to any strangers you write to or communicate with on the Internet. Never arrange to meet strangers who approach you whilst on the computer; anyone can pretend to be someone else. Someone pretending to be a friend may not have your best interests at heart*
- ✓ Treat others as they would expect to be treated, *e.g. show respect and be polite. Remember that something that may seem like a joke to you could upset someone else.*
- ✓ Always tell your teacher or another adult if you ever see, hear or read anything which makes you feel uncomfortable while using the Internet, e-mail or the Learning Platform
- ✓ Respect copyright and trademarks. *You cannot use the words or pictures that you see on an Internet site without giving credit to the person who produced the information originally. You must not copy text or pictures from the Internet and hand it in to your teacher as your own work.*

- ✓ Check with a teacher before:
  - sending e-mail
  - downloading files
  - completing questionnaires or subscription forms
  - opening e-mail attachments

You should not:

- X Send, access, store or display offensive or upsetting messages or pictures
- X Use or send bad, threatening or annoying language nor any language which might incite hatred against any ethnic, religious or other minority
- X Intentionally waste resources

Please note:

You should always log out and close your browser when your session has finished.

User areas on the school network will be closely monitored and staff may review your files and communications to maintain system integrity.

Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate. If applicable, external agencies may be involved: certain activities may constitute a criminal offence.

Oxfordshire County Council

APPENDIX 4

AN EXAMPLE OF AN E-LEARNING CODE OF CONDUCT FOR YOUNGER USERS

You should:

Always follow the instructions of your teacher.

Keep your username and password secret.

Always be nice and polite when you send messages to other users.

Always tell your teacher if you see, hear or read anything which makes you feel uncomfortable while using the computer.

You should not:

Send anyone a message which is not nice.

Use bad language in a message.

Use any other person's work or e-mail.

Tell a stranger any of the following information:

- your name
- your home address
- your telephone numbers
- any other personal information about yourself or any of your friends.

When you are finished using a computer you should always close it down properly following your teacher's instructions.

Oxfordshire County Council

APPENDIX 5

AN EXAMPLE OF A COPYRIGHT RELEASE STATEMENT

This school may produce printed publications and/or a school web site which may include examples of pupil's work and/or photographs of pupils. No child's work will ever be used without his/her permission and we take the issue of child safety very seriously which includes the use of images of pupils. Including images of pupils in school publications and on the school website can be highly motivating for the pupils involved, and provides a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils, which means that pupils must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents consent to the school publishing their children's work and to the taking and using of photographs and images of their children subject to strict confidentiality of personal information. (This can be changed at any time; please see the Headteacher or ICT Co-ordinator).

Oxfordshire County Council

APPENDIX 6

AN EXAMPLE OF REQUEST FOR PARENTAL AGREEMENT FOR USE OF DIGITAL VIDEO MATERIAL

Digital video is an exciting medium which can motivate and inspire pupils. Research has shown that using digital video in education can help encourage creativity, motivate and enthuse pupils, and improve communication and team-working skills.

At **[*school name*]** we intend to use digital video as part of our learning and teaching and for the recording of school productions and events.

We ask that parents consent to their child taking part in the production of digital video, and/or appearing in films.

Whereas the risks of using digital video in education are minimal, schools have a duty of care towards pupils. This means that pupils will remain unidentifiable, reducing the risk of inappropriate contact, if images or examples of their work (including digital video) are used on the school website. All digital video work at **[*school name*]** is underpinned by our acceptable use and internet safety policies.

Oxfordshire County Council

APPENDIX 7

FILTERING OPTIONS FOR SEARCH ENGINES

Most major search engines offer some type of filtering ability. This is intended to reduce the amount of inappropriate materials which teachers will not want children to encounter.

Google
www.google.co.uk
The default setting for Google filtering is moderate and it is set to exclude most explicit images from Google Image Search results. Teachers, at least in primary schools, should select the **strict filtering** option.

AllTheWeb
www.alltheweb.com
Use the Basic Settings page to enable the **Offensive Content Filter** option.

AltaVista
www.altavista.com
Use the **Family Filter** Setup page.

Ask Jeeves
www.ask.com
Use options for **Content Filtering** on the Your Settings page

Lycos
www.lycos.co.uk
Use the **Adult Filter** section of the Advanced Search Filters page

Yahoo
www.yahoo.co.uk
Set the **SafeSearch Filter** option via the Search Preferences page.

N.B. These filters are not perfect but used in conjunction with the LA level filters should help to provide a safe environment for pupils as far as it is possible.

Oxfordshire County Council

APPENDIX 8

SEARCH ENGINES SPECIFICALLY FOR CHILDREN

(WARNING - These sites allow easy navigation to teenage/young adult content on health matters and contain advertisements by various sponsors e.g. Pepsi, BUPA etc.)

Ask Jeeves for Kids (6-12 years)
www.ajkids.com

Yahooligans
www.yahooligans.yahoo.com/

KidsClick
www.sunsite.berkeley.edu/KidsClick!/

Kids-net Australia.
www.kids.net.au/

Oxfordshire County Council

Diocesan Schools Commission
Tel: 01675 430230 Fax: 01675 430321
Email: bdsc@bdsc.org.uk Web: www.bdsc.org.uk
See website for address