



Children's Services
Achievement and Inclusion Service

The Acceptable Use of ICT Systems in Harrow Schools

Advice and Guidance

28th January 2010

The Acceptable Use of ICT Systems (AUIS): establishing safe and responsible behaviours

“Children and young people need to be empowered to keep themselves safe – this isn’t just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim.”

Dr. Tanya Byron

Safer children in a digital world: The report of the Byron Review (www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf)

I Introduction

It is generally agreed that there is no present or foreseeable future technical solution that can consistently guarantee the preclusion of pupils and staff from access to, or contact from, unwanted Internet material. This includes racist, extremist, political or violent material. Neither are there guaranteed technical solutions to prevent the consequences of deliberate misuse of ICT systems, including ‘cyber-bullying’ and the loss of sensitive or highly valuable data. In these circumstances the reaction of schools to treat e-safety as an issue for education and parental involvement soon becomes the only sensible course.

For fuller descriptions of the issues related to e-safety, the use of ICT systems and the Internet please refer to the comprehensive advice and guidance from:

- The British Educational Communications and Technology Agency (Becta), www.becta.org.uk, particularly:
 - <http://www.becta.org.uk/publications/aupsincontext>, and
 - <http://www.becta.org.uk/safeguardinglearners>;
- The London Grid for Learning’s e-Safety advice and resources, <http://cms.lgfl.net/lgfl/web/safety>;
- UK Children Go Online, Prof. Sonia Livingstone and Magdalena Bober, London School of Economics, April 2005, www.lse.ac.uk/collections/children-go-online/UKCGO_Final_report.pdf;
- Safer children in a digital world: The report of the Byron Review, www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf;
- DCSF: National Strategies – Secondary, “Beyond The e-safety Net”, <http://nationalstrategies.standards.dcsf.gov.uk/node/173927>;
- Particularly helpful are the resources ‘Know IT All for Parents’ (in 9 languages), www.childnet-int.org/kia at Childnet International;
- Child Exploitation and Online Protection Centre (CEOP), <http://www.ceop.gov.uk/>;
- The National Association of Advisers for Computers in Education (NAACE), www.naace.org.

Balancing opportunities and risks

More skilled young people do not avoid the risks: not only do the most skilled young people fail to avoid on-line risks, but their risky encounters increase with increased use – thought these young people are more likely to be able to deal with the risks.

Opportunities and risks go hand in hand: there is a strong, positive association between opportunities and risks – the more children and young people experience the one, the more they also experience the other, and vice versa.

2 What are the risks?

The Byron Review classified the risks as relating to **content, contact** and **conduct**. The risk is often determined by **behaviours** rather than the technologies themselves (see **UK Children Go Online**, by Professor Sonia Livingstone and Magdalena Bober, The London School of Economics, published April 2005, (www.lse.ac.uk/collections/children-go-online/UKCGO_Final_report.pdf).

Behaviours, activities and their contexts					
	Commercial	Aggressive	Sexual	Values	Protective Actions
Content (child as the recipient)	Adverts, spam, sponsorship and personal information	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, racist and misleading information or advice	To what extent does the school's monitoring system (e.g. from Securus) help to protect pupils and staff in these categories of risk? (see Appendix A)
Contact (child as the participant)	Tracking and harvesting personal information	Being bullied, harassed or stalked and involvement with violent extremism	Meeting strangers and being groomed	Self-harm and unwelcome persuasions	
Conduct (child as the initiator)	Illegal downloading, hacking, gambling, financial scams and terrorism	Bullying or harassing another and the creation of violent extremism materials or communications	Creating and uploading inappropriate material	Providing misleading information/advice, e.g. misuse of social networking sites such as MyFace or YouTube	

Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review.

The misuse of schools' computer networks and other devices (including laptops, personal digital assistants, digital scanners, music players, mobile phones and other similar devices capable of storing and playing images, sounds and texts) for the transfer, storage and manipulation of pornographic or offensive images and texts is completely unacceptable. In some cases this will also be a criminal offence under the Computer Misuse Act 1990, whether within the school or not. In many cases, laws relating to copyright, libel, or incitement to racial hatred or extremism also apply as they would in other forms of communication.

Schools are **very strongly advised** to take all reasonable steps to discharge their duty of care towards their pupils and staff in this sensitive and complex area. A robust and regularly reviewed AUIS policy (and practice) that is implemented by all staff and pupils and monitored by senior leaders, will demonstrate how the school values their ICT systems and how their use impacts on the learning and teaching in the school. This should be included in the school's Ofsted SEF. There are also clear links to elements of Becta's Self Review Framework (SRF) that can lead to a school gaining the widely recognised and valued Becta ICT Mark.

In the unlikely event that a pupil's or teacher's use of the Internet and/or school ICT systems is unacceptable or criminal, it is important that the school, its management and the Council are not liable for any legal action as a consequence of the actions of these individuals. Please remember that your school management and board of governors are potentially liable to legal action until these procedures are implemented.

The extracts, which appear in the side bar, to the right, have been taken from the executive summary of the research **UK Children Go Online**, LSE, April 2005.

Access to the Internet

Socio-economic differences are sizeable: **88%** of middle class but only **61%** of working class children have accessed the Internet at home.

Many computers are located in private rooms: **19%** of children have Internet access in their bedroom.

The nature of Internet use

Most use it for searching and homework: **90%** of **9 – 19** year olds who go on-line daily or weekly use the Internet to do work for school or college and **94%** use it to get information for other things.

Some use it for less-approved activities: Among **12 – 19** year olds who go on-line daily or weekly, **21%** admit to having copied something from the Internet for a school project and handed it in as their own.

3 Summary of the sections, who might be involved and what to do next

The document replaces and updates the advice and guidance that was previously distributed to all Harrow schools. It contains draft school policies, letters for parents, procedure documents (including technical procedures to review and monitor the content of school computer systems), guidance for parents, and advice and guidance for governors. Please use them as the basis, after modification, for your own use.

The sections are:

A School Policy for The Acceptable Use of ICT Systems (AUIS); this will need to be constructed with additional material from the Appendices of this document.

Appendix A – Safeguarding: ICT and Ofsted; includes an audit tool that schools can use to quickly identify whether they fulfil the criteria that ensures that pupils feel safe and that schools know their pupils are safe.

Appendix B – Responsible Internet and computer use; examples of pupil and staff 'contracts', parent/carer permission letters, and guidelines for safe and responsible Internet use.

Appendix C – Technical support for ICT; information and pro formas that schools can use to ensure that their technical support systems provide sufficient security and reliability, and establish 'contracts' for the use of the Internet by pupils and staff.

Appendix D – Pupils Using Computers at Home; this section contains guidance and recommendations for a school's leadership team including aspects such as:

- planning a strategy and consulting governors and staff, as there are emotive issues for teachers involved;
- ensuring good access is available, through school or community, for those without ICT at home;
- informing parents about the school's approach to safe Internet access.

Appendix E – Sources of e-safety information for parents, carers and governors; this section provides information on printed resources, web sites and other on-line resources.

Appendix F – Using New Technology; hints and tips for adults working with children and young people.

Appendix G – The Use of digital and video images; advice and guidance about using images on a school web site and in other forms of publishing or communications.

Appendix H – Taking encrypted data overseas; advice from Becta and LGfL about avoiding problems when visiting other countries as part of school activities.

Appendix I – Managed Learning Environment (MLE) Administrator Confidentiality Agreement; advice about the maintenance of confidentiality of data held by the school's MLE.

Inequalities and the digital divide

Parents' experience of the Internet matters: daily and weekly users have parents who also use the Internet more often and are more expert.

The Internet is not yet used to its full potential: many children and young people are not yet taking up the full potential of the Internet, for example visiting a narrow range of sites or not interacting with sites.

Education, learning and literacy

Skills gap between parents and children: only 16% of weekly and daily user parents consider themselves advanced compared with 32% of children.

Children lack key skills in evaluating on-line content: 38% of pupils aged 9 – 19 trust most of the information on the Internet, and only 33% of 9 – 19 year olds daily and weekly users have been taught how to judge the reliability of on-line information.

Who should be involved in creating the AUIS policy?

- The ICT Co-ordinator.
- The E-Safety Co-ordinator.
- The computer network manager / technician(s).
- Senior leaders with a responsibility for ICT.
- Subject and/or aspect leaders as appropriate.
- A representative group from the school's Pupil Council; and eventually.
- A sub-group of the Governing Body that may include parent representation.

What might happen next?

- 1 A 'task group' from those identified above should be convened by the headteacher and a task group leader identified.
- 2 The draft document should be considered against the school's existing policies and guidance.
- 3 Using this draft document as the standard, review the school's existing policies and guidance; where the school's documentation is at least as robust as that in the draft document, the school could retain their existing documents with minor amendments.
- 4 If there is no matching policy or guidance, or the existing policy and guidance is deemed to be insufficiently robust, the task group should prioritise the adoption of the draft policies and guidance for the school; specific sections could be allocated to specific staff. The adoption of Appendixes A and B might be priorities.
- 5 At this point, the sub-group of the Governing Body could be brought into the process and the draft documents discussed with them. The monitoring and management responsibilities identified in the draft policy and guidance document will need to be considered and some job descriptions may need adjustment.
- 6 Throughout this process the whole staff and, where relevant the pupils, should be involved in discussing and agreeing the changes and amendments recommended by the task group.
- 7 The school's draft policies and guidance should then be tabled at the earliest Governing Body meeting for adoption as agreed school policy and practice.
- 8 At the earliest opportunity all staff, pupils and parents should be encouraged to play their part as 'partners' in engaging with the school's new policies and practice.

Communication

The mobile phone is the preferred method of communication: whether for passing time, making arrangements, getting advice, gossiping or flirting, the phone and text messaging are preferred over emailing or instant messaging.

Some seek advice on-line: 25% of 12 – 19 year old daily and weekly users say they go on-line to get advice.

Participation

Producing as well as receiving content: 44% of 9 – 19 year old weekly users have completed a quiz on-line, 25% have sent an email or text message to a website, 22% have voted for something on-line, and 17% have sent pictures or stories to a website.

Age, gender and social grade make a difference: girls, and older and middle class teens visit a broader range of civic and political sites.

4 A Policy for the Acceptable Use of ICT Systems (AUIS)

This section provides suggested statements for schools to add to and edit. It is based on the original work of Kent County Council (www.kent.gov.uk/eis).

The school's policy should be built on the following five core principles:

- 1 **Guided educational use** – access to and the use of the Internet should be planned, purposeful and have educational value.
- 2 **Risk Assessment** – schools should be fully aware of the risks and know how to respond when:
 - a) pupils and staff come across inappropriate material;
 - b) misuse of ICT is discovered.
- 3 **Responsibility** – all users of the school's ICT systems must take responsibility for their use; the balance between educating pupils (and possibly staff) to take a responsible approach and the use of regulation and technical solutions must be carefully judged.
- 4 **Regulation** – the use of a finite and expensive resource that can be misused requires some regulation; fair rules, clearly and prominently displayed, will help users make responsible decisions.
- 5 **Appropriate strategies** – strategies should be selected to suit the school situation and predictable problems likely to arise, and their effectiveness monitored; there is no straightforward or totally effective solution; staff, parents and pupils must remain vigilant.

4a Who will write and review the policy?

Possible statement:

The school has written our Internet Policy, building on LA and government guidance. It has been agreed by senior management and approved by governors (and the PTA if appropriate). It will be reviewed annually.

Created by: Date:

To be revised: Approved:

4b Why ICT systems, devices and the Internet are important to our pupils and staff

Possible statements:

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

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

ICT and Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

Using ICT and the Internet are essential elements of 21st century life. The school provides all learners with quality ICT systems and Internet access as part of their learning experience.

The risks of undesirable content

More than half of 9 – 19 year olds have seen pornography on-line: 57% of daily and weekly users have come into contact with on-line porn.

Most pornography is viewed unintentionally: 38% have seen a pornographic pop-up advert while doing something else, 36% have accidentally found themselves on a porn site when looking for something else, and 25% have received pornographic junk mail.

The risks of on-line communication

Parents underestimate children's negative experiences: one third of 9 – 19 year old daily and weekly users have received unwanted sexual (31%) or nasty comments (33%) on-line or by text message, though only 7% of parents are aware that their child has received sexual comments and only 4% that their child has been bullied on-line.

Children divulge personal information on-line: 46% say that they have given out personal information to someone that they met on-line.

4c How do ICT systems and the Internet benefit education?

The statement of benefits might include:

Through:

- access to world-wide educational resources including museums and art galleries;
- access to the school's MLE and the London Grid for Learning (LGfL);
- educational and cultural exchanges between pupils;
- cultural, vocational, social and leisure use in libraries, clubs and at home.
- access to experts in many fields for pupils and staff;
- CPD through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DCSF;
- mentoring of pupils and provide peer support for them and teachers.

4d How will the Internet enhance learning?

Possible statements:

The school's Internet access is designed expressly for pupil and staff use and will include appropriate filtering and monitoring.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities.

Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be taught how to use the Internet for research, including the skills of knowledge location, retrieval and evaluation.

The school will use and develop the on-line content available through the LGfL and our MLE.

As much as possible, the school's chosen Internet service provider has organised information resources in ways that point pupils to those that have been reviewed and evaluated prior to use. While pupils may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Pupils may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

A parental wish list

More education: 75% want to see more and better teaching and guidance in schools while 67% want more and better information and advice for parents.

Improved technology: 66% want improved filtering software, 54% improved parental controls and 51% improved monitoring software.

Access to the Internet

Home access is growing: 75% of 9 – 19 year olds have accessed the Internet from a computer at home. Homes with children lead in gaining Internet access: 36% have more than one computer at home, and 24% live in a household with broadband access.

4e How will pupils learn to evaluate Internet content?

Schools are **strongly recommended** to read and reflect on the teaching strategies set out in two of Becta's publications:

- "Signposts to safety, Teaching e-safety at Key Stages 1 and 2", 2007, <http://publications.becta.org.uk/display.cfm?resID=32422>;
- "Signposts to safety, Teaching e-safety at Key Stages 3 and 4", 2007, <http://publications.becta.org.uk/display.cfm?resID=32424>.

Incorporate relevant materials from the e-safety section of the LGfL web site, (<http://cms.lgfl.net/lgfl/web/safety>).

Receive CEOP's termly newsletter, (<http://www.ceop.gov.uk/> and register on-line).

Possible statements:

If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider (ISP) by the ICT or E-Safety Co-ordinator.

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils will be taught the 'green cross code for the Internet' – '*Zip it, Block it, Flag it*'. Details are available at UKCCIS, <http://www.dcsf.gov.uk/ukccis/>.

The following will need adaptation according to the pupils' age:

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its validity.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Training will be available to staff in the evaluation of web based materials and methods of developing pupils' critical attitudes.

4f How will email be managed?

Possible statements:

Pupils may only use approved email accounts on the school system, e.g. LondonMail or SafeMail for pupils and (both from LGfL).

School staff will use the secure StaffMail system available through LGfL.

Pupils will immediately tell a teacher if they receive offensive email.

Pupils will not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.

Whole-class or group email addresses will be used at KS2 and below.

Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and may be restricted.

Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

Staff will not attach unencrypted sensitive data to emails.

If sensitive data has to be sent over the Internet it will be sent via the USO FX System from LGfL.

The school's MLE, will be used to temporarily store reports to parents during the writing process; the files will not be transported by portable storage devices.

Communication

Most on-line communication is with local friends: being in constant contact with friends is highly valued, and there is little interest contacting strangers, though some have contacted people that they have not met face to face, this being mainly among the 21% who visit chat rooms.

The risks of undesirable content

Too young to have seen it: 45% of 18 – 19 year old Internet users who have seen any pornography (on or off-line) think they were too young to have seen it when they first did. Other areas of concern: 22% of 9 – 19 year old daily and weekly users have accidentally ended up on a site with violent or gruesome pictures and 9% on a site that is hostile or hateful to a group of people.

4g How will the school's MLE and web site be managed?

See also Appendix I for advice about the MLE administrator's role.

Possible statements:

The point of contact on the web site will be the school address, school email and telephone number. Staff or pupils' home information will not be published.

Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the web site or MLE, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site or MLE.

The headteacher or nominee takes editorial responsibility and ensure that e-content is accurate and appropriate.

The web site and MLE will comply with the school's guidelines for publications.

The copyright of all material will be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Staff will ensure that all materials used within the MLE will have been carefully selected for their teaching and learning value.

Editorial control of subject or year group pages within the MLE will be passed to teachers; they will be expected to exercise this control with care and all due regard for their position of trust and duty of care.

4h Regulation of chat, newsgroups, RSS feeds and email lists

Possible statements:

Newsgroups and email lists will not be made available to pupils unless an educational requirement for their use has been demonstrated.

Pupils will not be allowed access to public or unregulated chat rooms.

Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

RSS feeds will be available through the MLE provided users can demonstrate a good educational benefit from using them.

4i How will emerging technologies be managed?

Possible statements:

Risk assessments will be carried out before pupils and staff are allowed to use new technologies in school.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones (or similar mobile devices that can access the Internet, record and transmit text, sound, images, etc.) will not be used during lessons or formal school time. The recording and sending of abusive or inappropriate text messages, sounds or images (still or moving) is forbidden.

The school does not permit the use or activation of digital, electronic, or other recording technologies to be used on school premises except those devices that are for the clear and direct use by teachers, and pupils with a teacher's permission, to facilitate pupils learning.

The risks of undesirable content

There is more porn on the Internet than in other media: moreover, 53% of parents consider (and children agree) that the Internet is more likely to expose children to pornography than are television, video or magazines.

The risks of on-line communication

Children engage in identity play: 40% say that they have pretended about themselves on-line. Some have attended face to face meetings: 30% have made an on-line acquaintance, and 8% say they have met face to face with someone whom they first met on-line.

4j How will Internet access be authorised?

Possible statements:

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, e.g. staff may leave or a pupil's access be withdrawn.

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents will be informed that pupils will be provided with supervised Internet access.

High school pupils must apply for Internet access individually by agreeing to abide by the Responsible Internet Use statement.

Parents will be asked to sign and return a consent form (perhaps based on the examples on pages 22 and 23).

Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.

4k How will the risks be assessed?

Possible statements:

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the nature of Internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be regularly reviewed.

The headteacher will ensure this policy is implemented and compliance is monitored.

4l How will filtering be managed?

The technical strategies to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

Blocking strategies prevent access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day.

A walled-garden or allow list provides access only to a list of approved sites. An allow list will inevitably restrict pupils' access to a narrow range of information.

Dynamic filtering examines the content of Web pages or email for unsuitable words. Filtering of outgoing information such as Web searches is also required.

Rating systems give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.

Monitoring records Internet sites visited by individual user. Access to a site forbidden by the filtering policy will result in a report. It is also possible to remove access automatically after a set number of policy violations.

Regulating the Internet at home

Parents seek to manage their children's Internet use: most parents, whose child has home access to the Internet, claim that they directly share in and/or support their child on the Internet, though their children are less likely to say that this occurs.

Parents face some difficult challenges: 18% of parents say they don't know how to help their child use the Internet safely.

Regulating the Internet at home

Confusion about filtering: in homes with Internet access, 35% of children say that filtering software has been installed on their computer while 46% of parents claim this.

Possible statements:

The school will work in partnership with parents, the LA, the DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL and content will be reported to the Internet Service Provider by the ICT Co-ordinator or network manager.

The school will establish its own filtering criteria in addition to the default settings (larger schools might manage the configuration of their filtering; this task requires both educational and technical experience).

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal will be referred to our ISP, LGfL, the *Internet Watch Foundation* (www.iwf.org.uk) and other appropriate agencies.

The school, in discussion with the filtering provider, will select filtering strategies where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

4m How will the policy be introduced to pupils?**Possible statements:**

Rules for Internet access will be posted in all rooms where computers are used.

Pupils will be informed that Internet use will be monitored.

Instruction in responsible and safe use should precede Internet access.

A module on responsible Internet use will be included in the PSHE programme covering both school and home use.

4n How will staff be consulted?**Possible statements:**

All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.

Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

The monitoring of Internet use is a sensitive matter. Adults who operate monitoring procedures should be supervised by senior management.

Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

Regulating the Internet at home

Children don't want restrictions: **69%** of 9 – 17 year old daily and weekly users say they mind their parents restricting or monitoring their Internet use.

Children protect their privacy from parents: **63%** of 12 – 19 year old home Internet users have taken some action to hide their on-line activities from their parents.

Regulating the Internet at home

Mind the gap: there are considerable gaps in understanding between parents and children (in Internet expertise, in awareness of risks and in acknowledgement of domestic regulation implemented) which impede an effective regulation of children's Internet use within the home.

4o How will the security of the ICT system be maintained?

Possible statements:

The school ICT systems will be reviewed regularly.

Virus protection will be installed and updated regularly.

Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.

Personal data sent over the Internet will be encrypted.

Use of portable storage media such as USB memory sticks, DVDs, CD-ROMs and other storage devices will be reviewed. Where applicable such devices will comply with latest guidance on Handling Sensitive Data. At the very least, USB and portable drives used to store sensitive data will comply with FIPSI 40-2 Standard (which includes the AES 256 standard).

Portable media may not be brought into school without specific permission and a virus check.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.

Files held on the school's network will be regularly checked.

4p How will complaints regarding Internet use be handled?

Possible statements:

Responsibility for handling incidents will be delegated to a senior member of staff.

Complaints about staff misuse will be referred to the Headteacher.

Pupils and parents will be informed of the complaints procedure.

Parents and pupils will work in partnership with staff to resolve issues.

As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Sanctions available include:

- interview / counselling by Head of Year;
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

4q How will the school engage with, and positively encourage, parents as partners?

Possible statements:

Parents' attention will be drawn to this Policy in newsletters, the school brochure and on the school Web site.

Issues will be handled sensitively to inform parents without undue alarm.

A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

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

Interested parents will be referred to organisations such as:

- Childnet International (www.childnet-int.org/kia);
- the Parent's page of Directgov (<http://www.direct.gov.uk/en/Parents/index.htm>);
- *Parents Online* (www.parents.org.uk); and
- *NCH Action for Children*, (www.nch.org.uk).

Balancing opportunities and risks

Internet literacy is crucial: increasing Internet skills is vital since it seems that children and young people's level of on-line skills has a direct influence on the breadth of on-line opportunities and risks they experience.

A parental wish list

Stricter regulation: 85% of parents want to see tougher laws on on-line pornography, with 59% wanting stricter regulation of on-line services.

4r How is the school's ICT system used across the community?

Possible statements:

Adult users will need to sign the acceptable use policy.

Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child.

In the Library, generally children under 8 years of age will be accompanied by an adult when accessing the Internet.

4s Videoconferencing

Possible statements:

The equipment and network:

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer; the equipment must be secure and if necessary locked away when not in use.
- The use of a reliable service – *Click to Meet* from LGfL – will be used.
- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users:

- Pupils will ask permission before making or answering a videoconference call; all videoconferencing sessions will be supervised.
- Parents and guardians should agree for their children to take part in videoconferences.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

Content:

- When recording a lesson, all sites and participants should give written permission. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material to be stored securely with authorised access.
- If third-party materials are included the school will not infringe the owner's Intellectual Property Rights (IPR).
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check they are delivering material that is appropriate for your class.

4t Search engines and inappropriate images

When using a search engine for images users will often find inappropriate pictures. Some may be pornographic, some offensive in their representation of various groups of people and some will be inappropriate when related to pupil's age. Even with filtering and 'safe search' options, there will be instances when pupils and/or staff will find inappropriate images. Schools will want to educate pupils in the responsible use of images and visual literacy.

Possible Statements:

Access to images will be restricted by using the 'safe search' option within the search engine, although this is not completely safe.

Google (or similar search engine) images will be not be available to pupils and staff (this is more secure but denies pupils and staff access to wealth of good educational images).

Google (or similar search engine) images will be made available through the use of more a secure search option provided by LGfL (this will need to be activated in each school – contact the LA at Harrow Teachers' Centre).

Images from child friendly sites (e.g. Yahoo!igans) will be used.

Summary of recommendations

Recognise the complexity of 'access' when designing information and advice campaigns.

Direct children and young people towards valuable content.

Address the changing conditions of digital exclusion.

Improve levels of Internet literacy.

Develop critical evaluation skills.

4u Use of digital and video images (see also Appendix G)

Possible Statements:

Procedures and practice will ensure website safety.

A senior member of staff will oversee / authorise the website's content and check suitability.

The school will not use the first name and last name of individuals in a photograph:

- If the pupil is named, we will avoid using their photograph / video footage;
- If the photograph /video is used, we will avoid naming the pupil.

The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained.

Uploading of information is restricted to X administration officer / X Teaching Assistant / all class teachers in their class areas / etc.

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

The point of contact on the web site is the school address and telephone number. Home information or individual email identities will not be published.

We will ensure that before any images are uploaded to our web site or published electronically they are re-named so that the name of the pupil cannot be read by right-clicking on the image.

We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication.

We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website.

We do not include the full names of pupils in the credits of any published school produced video materials / DVDs.

Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.

Pupils are only able to publish to their own 'safe' area on the MLE.

Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

Pupils are taught about how images can be abused in their e-safety education programme.

Summary of recommendations

Develop on-line advice resources with the help of young people.

Facilitate the shift from just receiving to also creating content.

Rethink on-line participation from 'having your say' to 'being listened to'.

Continue efforts to prevent exposure to undesirable content.

Maintain Internet safety awareness.

4v Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

Possible Statements:

The schools will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends, specific interests and clubs etc.

Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be strongly advised not to run social network spaces for student use on a personal basis.

Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Students will be strongly advised not to publish specific and detailed private thoughts (schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments).

4w Taking encrypted data overseas (see Appendix H)

Schools should always check current restrictions before leaving the UK with encryption software or encrypted data. When travelling to countries where encryption is permitted, it is still good practice to store encrypted data on media, laptops or mobile devices in a hotel room safe.

Possible Statements:

The school will not take the device on a visit (preferred).

The will remove any encryption software and encrypted data from your laptop or mobile device (which will have support implications or breach the UK's own guidelines on information security).

The school will apply in advance for the appropriate licence before leaving the UK.

Summary of policy recommendations

Encourage parental sharing in children's Internet use.

Respect children's on-line privacy in the home.

Take care not to reduce young people's on-line opportunities.

Target guidance and regulation more carefully at different groups of children.

Design websites which encourage Internet literacy.

Develop more and better child and youth portals.

Appendix A – Safeguarding: ICT and Ofsted

Is your school e-safe?

1 Ofsted summarises Safeguarding as:

- protecting children and young people from maltreatment;
- preventing impairment of children and young people's health or development;
- ensuring that children and young people are growing up in circumstances consistent with the provision of safe and effective care;
- undertaking that role so as to enable those children and young people to have optimum life chances and to enter adulthood successfully.

2 Safeguarding includes issues for schools such as:

- **pupils' health and safety;**
- **bullying;**
- **racist abuse;**
- **harassment and discrimination;**
- use of physical intervention;
- meeting the needs of pupils with medical conditions;
- providing first aid;
- drug and substance misuse;
- educational visits;
- intimate care;
- **Internet safety;**
- **issues specific to a local area or population**, e.g. gang activity;
- **school security.**

3. Ofsted makes these two key judgements:

- To what extent do pupils **feel** safe?
- To what extent does the school **know** the pupils are safe?

4. Audit tool

On the next page you will find an auditing tool that aims to help schools quickly gain an overview of the various aspects of Safeguarding related specifically to ICT.

The web sites refer to sources of information and advice that schools may find helpful in ensuring that each of the safeguarding aspects is fully in place.

5. Risks analysed

On page 3 you will find a grid showing how the behaviours of pupils in three contexts might help all school staff more fully understand the various types of behaviours involved. The references to the Livingstone and Byron reports are included for further reading.

	Safeguarding Aspect	Fully in place	In place: needs review	Partially in place	Not in place	Sources of information and notes
Does the school:	have a nominated E-Safety Co-ordinator?					Member of the leadership team.
	audit its e-safety measures?					LGfL: http://cms.lgfl.net/igfl/web/safety National Education Network: www.nen.gov.uk/esafety
	have a robust Acceptable Use of ICT Systems Policy (AUIS)?					LB – Harrow AUIS Policy (this document) Becta: www.becta.org.uk/publications/aupsincontext
	include e-safety in your Ofsted Self Evaluation Form (SEF)?					SEF sections A2.5, A3.4, A4.7 (in particular), C16 and C29
	keep an incident log and monitor your measures?					See below for advice on monitoring and alerting Securus: www.securus.co.uk Forensic: www.synetrix.com
	handle cyber bullying issues well?					Digizen: www.digizen.org/cyberbullying Teacher-net: www.teacher.net.gov.uk
	raise awareness of the issues, e.g. through holding assemblies?					Thinkuknow: www.thinkuknow.co.uk/teachers
	use Becta's Self Review Framework (SRF) to audit, evaluate and monitor this aspect?					Becta: https://selfreview.becta.org.uk
	understand what safe and responsible online behaviour means?					Where are they taught about the issues? Who monitors this? Do you use Becta's Self Review Framework (SRF) to help audit this aspect? LGfL: http://cms.lgfl.net/igfl/web/safety
	receive e-safety education at appropriate places across the curriculum?					Signposts to safety: www.becta.org.uk/publications Kidsmart: www.kidsmart.org.uk Thinkuknow: www.thinkuknow.co.uk/publications
have sufficient opportunities to improve their digital literacy skills?					Do pupils have opportunities to contribute to the school's MLE / Web Site?	
know the Safe, Meeting, Accepting, Reliable, Tell (SMART) rules?					Kidsmart http://www.kidsmart.org.uk/ Childnet: www.childnet.com	
know how to report any concerns they may have?					CEOP: www.ceop.gov.uk/reportabase/index.asp	

Safeguarding Aspect	Fully in pace	In place: needs review	Partially in place	Not in place	Sources of information and notes
Do all staff:	understand e-safety issues and risks?				Childnet: www.childnet.com/kia Thinkuknow: www.thinkuknow.co.uk/teachers Becta: www.becta.org.uk/schools/communities/safetynet
	receive regular training and updates?				DCSF: National Strategies – Secondary, “Beyond The e-safety Net”, http://nationalstrategies.standards.dcsf.gov.uk/node/173927
	know how to escalate an issue of concern?				Discussions with staff and the member of staff particularly responsible for child protection
	know how to keep data safe and secure?				Becta: www.becta.org.uk/schools/datasetsecurity
	know how to protect themselves online				Teachernet: www.teachernet.gov.uk TeachToday: www.teachtoday.eu LGfL: http://cms.lgfl.net/lgfl/web/safety
	know how to conduct themselves professionally online?				Every Child Matters: www.everychildmatters.gov.uk/resources-and-practice/IG00311
	know about the updated e-safety guidance for QTS standard Q21: Health and well-being?				TDA: www.tda.gov.uk/partners/ittstandards/guidancej38/qts.aspx
	understand e-safety issues and risks?				NGA: www.nga.org.uk/uploads/documents/NGA-Becta%20Sept.pdf LGfL: http://cms.lgfl.net/lgfl/web/safety
	understand their roles and responsibilities?				Have they been involved with any whole staff training days or other opportunities?
	receive regular training and updates?				thinkuknow: www.thinkuknow.co.uk/parents
Do your Parents & Governors:	understand how to protect their children in the home?				Know it all: www.childnet.com/kia Thinkuknow: www.thinkuknow.co.uk/parents Directgov: www.direct.gov.uk
	know how to report any concerns they may have?				CEOP: www.ceop.gov.uk/reportabase/index.asp

Safeguarding and ICT

There are a number of ICT related contexts in the Safeguarding element of the current Ofsted inspection framework:

- bullying;
- racist abuse;
- harassment and discrimination;
- educational visits;
- intimate care;
- Internet safety;
- issues specific to a local area or population, e.g. gang activity;
- school security.

Becta is strongly encouraging schools to keep an incident log and monitor the measures they have put in place to help them know their pupils are safe and as well as feel safe. Computers, their hard disks and similar devices should be treated similarly to school lockers. User's files and communications may be reviewed to ensure the ICT system is used responsibly. They should not expect files stored on school servers or disks to be private. As part of the monitoring process all schools are strongly recommended to adopt the following advice.

Monitoring and Alerting Procedures

The purpose of such procedures is to ensure that:

- pupils remain as safe as possible;
- pupils **feel** safe and schools can be more confident that their the pupils **are** safe;
- staff use the ICT resources safely and in a professional manner;
- schools' ICT systems are not abused.

The presence on the school's computer network, or portable computers provided to staff, of any unacceptable videos, sound recordings, images, emails, voice messages or texts should be immediately reported to a person designated by the headteacher. If these files are of such concern (for example, they clearly involve minors) and their source and location indicate deliberate or knowing staff or pupil misuse of the system, the headteacher (or the designated member of staff for child protection) must be informed, the computer shut down, securely isolated and the matter reported to the LA's Child Protection Officer without delay.

If, however, the unacceptable images, emails or texts are judged to be the consequence of *accidental* or *unknowing* use of the system, these files should be immediately and permanently removed from the hard disks concerned. This should be carried out by a person designated by the headteacher in the presence of another person. If, however, the images, emails or texts clearly involve minors the computer must be shut down, securely isolated and the LA's Child Protection Officer must be informed immediately.

To help schools monitor this aspect of Safeguarding schools should either:

- buy and install 'black box' from Securus (www.securus-software.com) or Policy Central (<http://forensicsoftware.co.uk>) to monitor user's use of their ICT systems or;
- buy a service from their technical support company based on one of the 'black box' systems or;
- buy an on-line service from, for example, Synetrix Ltd. that is one of the companies used by LGfL (www.synetrix.co.uk).

Whichever method is adopted, the school should be clear about:

- who will install and maintain the technology in the school;
- how the service will collate and report the incidents detected by the technology;
- to whom and with what frequency this reporting will be made.

Schools should implement the following ‘triggers’ of their monitoring system:

- images or videos of a pornographic nature (images are only discovered when there are inappropriate words on the same screen);
- images of weapons or drugs (including, for example, Samurai sword or dagger);
- images of a violent or extremely distasteful nature;
- sentences of a sexual nature or referring to matters concerning sex or acts of sex (these are most frequently found in instant messenger type programs);
- users:
 - searching for information about issues or products of a sexual, medical or personal nature;
 - searching for pictures of a sexual nature (the filtering usually blocks the attempt);
 - (mainly pupils) making rude or insulting remarks or statements about other people;
 - (mainly pupils) making threats of various kinds;
 - trying to bypass the Internet filtering or PC security;
- use of words associated with gambling;
- use of words associated with drugs.

The security and monitoring processes for staff laptops

This monitoring process is especially important when laptops are connected to the school’s computer network, either by cable or wireless technology, and thus have access to the Internet. This connection to the network also enables the movement of files from the laptop to the network and/or the school’s Managed Learning Environment (MLE) and vice versa.

Equally important, but requiring sensitive negotiation will be the review and monitoring of staff laptops that are permitted to access the Internet at home as well as at school. When connected to the Internet via the school’s network, the laptops will be subject to the filtering and restrictions that apply to the network. However, when the laptops connect to the Internet at home the filtering and restrictions may not apply and access to undesirable sites can occur.

Schools should, as a matter of urgency, implement a clear policy about the use of staff laptops and what will be acceptable use or not. Schools leaders will also need to be very clear as to the consequences of either decision. It is strongly advised that staff sign a paper copy of the conditions that relate to the school provision of a laptop. The wider the agreed uses of a staff laptop outside of school, the greater the number of violations that are likely to occur, may therefore be reported to senior staff and will require attention.

The configuration of monitoring systems and reporting of violations:

- the log on screen on all computers and laptops should tell users that the monitoring system is active and they are expected to adhere to the safe use policy;
- all libraries should be enabled;
- the default word list for each library should be enabled;
- to reflect the particular needs of the curriculum, schools should discuss with their technical support company, or those setting up the system, which additional words should to be added to the libraries;
- the headteacher (or nominated member of staff) should receive monthly reports from the system, even if there are no violations to report;
- the reports should be systematically evaluated for patterns of use so that the ICT system can be configured to provide maximum educational benefit whilst ensuring safe usage to pupils and staff.

Advice and guidance for network managers and/or technical support companies

Schools should either establish procedures with the school's own technicians or extend, or modify, the school's existing contract with their technical support company so that:

- the school's access to the Internet is filtered by an accredited service provider (e.g. via the school's connection to LGfL) and that the Internet Content Filtering Tool (ICFT) is regularly updated with the latest definitions;
- a list of sites to which access is blocked at both school level and at service provider level is established and maintained. This will enable a list of sites that are judged to be beneficial for learning and teaching to be accessed more quickly. These procedures will require the school to work in partnership with their technical support provider and discuss how best the lists can be managed. The use of a monitoring system, e.g. from Securus, will inform this process.
- at least three times a year the school should carry out (or have their technical support company carry out) a selective search of the physical hard disks of servers, desktop PCs and staff laptops to monitor and review stored images. Schools could select a percentage of each pupil year group to review and all staff accounts should be reviewed. The times of these reviews could be selected randomly or when other occurrences, such as pupils exchanging user names and passwords or unauthorised attempts to access the computer network, are discovered. Again, the use of a monitoring system, e.g. from Securus, will inform this process.
- using the outcomes from the evaluation of reports from a monitoring system, e.g. from Securus, select a reasonable number of users to have their:
 - Internet access history reviewed and tied with users and sessions; the history logs that exist to monitor activity should be reviewed as part of this process (schools could select a percentage of each year group and staff accounts to review);
 - email folders reviewed (schools could select a percentage of each year group and staff accounts to review);
 - Internet Options/history checked.

Anti-virus and Spyware software

It is **essential** that all school laptops have good quality **anti-virus and spyware software** installed on their hard disks. Protection from viruses can be achieved by using the free LGfL provided anti-virus software called *Sophos*. Schools are very strongly recommended to have this installed on all their laptops, especially staff laptops. Anti-spyware software should also be installed on laptops and regularly updated through a subscribed service. Schools should discuss this with the technical support company or in-house ICT support team.

Physical security of the computer network server

The server(s) should be located in a lockable, well ventilated, or air-conditioned room. There should be enough space for the ICT co-ordinator and technician to work at the computer attached directly to the server. If possible, a telephone should be available in the room for contacting the school's technical support partner or for complex problems requiring support from outside agencies.

Schools should seriously consider the recording and monitoring of physical access to the network server. This action would contribute to the ability of senior managers to both limit access to a known and 'accredited' number of people, and identify the timing of any undesirable use of the system.

Appendix B – Responsible Internet and computer use

Parents' permission letter – draft text

Xth/st/rd/nd Month 201X

Dear Parent,

Acceptable use of the Internet and ICT permission form

As part of the school's ICT programme we offer pupils supervised access to the Internet, the global network of computers you will have read about and seen on television. The school's speed of access to this network has recently been upgraded and is now at a very high speed.

Before being allowed to use the Internet and our ICT systems, all pupils must obtain parental permission. I invite you to sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet through the school's ICT system will enable our pupils to explore thousands of libraries, databases and similar pages of information while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet and computer use is to improve learning and teaching, pupils may find ways to access other materials as well. However, we believe that the benefits to pupils from access to the Internet exceed the disadvantages. But ultimately, parents and guardians are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end the school supports and respects each family's right to decide whether or not to apply for access.

During the school day, teachers will guide pupils toward appropriate materials and acceptable use of computers. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, films, radio and other carriers of potentially offensive media.

We would be grateful if you could read the enclosed guidance documents and then complete the permission form that follows.

Yours sincerely,

X

Headteacher

Xxx School

Pupil's Internet and school network permission form (201X)

Please complete and return this form to the headteacher.

Pupil statement

As a school user of the Internet and other computers, I agree to comply with the school rules on its use. I have read these rules that are included with this form and will use the network in a responsible way. I will observe all the rules explained to me by the school.

Pupil's Signature: _____ Date: ___ / ___ / 201x

Parent / guardian statement

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be unacceptable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Parent Name: _____

Parent Signature: _____ Date: ___ / ___ / 201x

Name of Pupil: _____

Form class: _____

Home Telephone: _____

Mobile Telephone: _____

Pupil guidelines for Internet and ICT use

Secondary schools

Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor.

The Internet is provided for pupils to conduct research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the agreements they have signed.

Computer storage areas, USB drives and portable storage devices will be treated like school lockers. Staff may review files and communications to insure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, films, radio and other potentially offensive media.

The following are not permitted (each is seen as having equal importance):

- 1 Storing, sending or displaying offensive messages or pictures (still or moving) using the school's computer network, PDAs or mobile phones.
- 2 Bringing into school portable storage media, mobile phones, PDAs, or similar devices containing unacceptable text, images (still or moving) or sounds.
- 3 Using obscene language.
- 4 Harassing, insulting or attacking others.
- 5 Inciting or promoting extremist racial behaviour.
- 6 Damaging computers, computer systems or computer networks.
- 7 Violating copyright laws.
- 8 Using other user's passwords.
- 9 Trespassing in other user's folders, work or files.
- 10 Intentionally wasting limited resources.

Sanctions

- 1 Violations of the above rules will result in a temporary or permanent ban on Internet or computer network use.
- 2 Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- 3 When applicable, police or local authorities may be involved.

Rules for responsible Internet and computer network use

Primary Schools

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only use the system with my own username and password, which I will keep secret;
- I will not look at other people's files;
- I will only use the computers for school work and homework;
- I will not bring in portable storage media from outside school unless I have asked my teacher;
- I will ask permission from my teacher before using the Internet;
- I will only email people I know or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet anyone, unless I am really sure that my parent(s), carer(s) have given permission;
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files and may look at the Internet sites I visit.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet or computer network use.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.

Staff use and guidelines

The computer network and school funded portable computers are owned by the school and are made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Policy for the Acceptable use of ICT Systems has been drawn up to protect all parties – the pupils, the staff, and the school.

- Irresponsible use may result in the loss of Internet access.
- The school reserves the right to examine or delete any files that may be held on its computer network or portable computers or to monitor any Internet sites visited by staff and pupils.
- Staff and pupils requesting Internet access and use of the school's computer network should sign a copy of this Acceptable Internet and ICT Systems Use Statement and return it to the school administration office.
- All Internet activity should be appropriate to staff professional activity or the pupil's education;
- Access should only be made via the authorised username and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for email sent and contacts made that may result in email being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected and sources acknowledged when used;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

Appendix C – Technical Support

Schools should aim to develop a stable, secure and reliable ICT infrastructure that is always available when it's needed by all users. With the increasing reliance that schools place on their already complex and growing computer systems a strategy for efficient and effective ICT management and support that – a technical support strategy – becomes even more important.

Teaching, learning and smooth administration cannot be successfully implemented without this technical reliability. Technical support for ICT should be pro-active, minimising the occurrence of failure as far as possible, protect the system against accidental or deliberate misuse, and, when things do go wrong, restoring the service to the users as quickly as possible.

This section provides information and pro forma that schools can use to:

- create a framework for technical ICT support by using on-line materials;
- use Becta's Technician's Competency Framework to review the readiness of their technical support partner or in-house team to meet the challenges of supporting the school's ICT systems;
- check their current technical support systems provide sufficient security and reliability;
- establish a policy for the acceptable use of the Internet by pupils and staff;
- extend the checks and monitoring of their ICT systems to prevent the misuse of their ICT systems.

Framework for ICT technical support

Becta has published a framework for ICT Technical Support (FITS at www.becta.org.uk/tsas) that deals with the wider issue of technical support in schools. At the outset of developing a technical support strategy, it's important to address the three key aspects:

1. There are a number of processes involved in providing technical support. Some are reactive and deal with faults as they occur; others are pro-active, aimed at preventing faults in the first place or generally improving the service.
2. The term 'processes' means actions such as identifying, logging, investigating, diagnosing and resolving a fault on a computer system – that whole process, from start to finish.
3. The Framework for Technical Support is a practical tool kit of advice, checklists and downloads for schools of any size or ICT proficiency.

The framework defines 10 processes that technical support should be able to carry out.

- Establish a 'service desk': the single point of contact within the school for all users of ICT.
- Incident management: quickly fix faults by restoring the ICT service to the user.
- Problem management: detect the underlying cause of faults and apply a permanent fix.
- Change management: manage and record the introduction of ICT changes.
- Release management: plan, test and manage the implementation of software and hardware.
- Configuration management: implement and maintain up-to-date records of ICT hardware and software.
- Availability and capacity management: carry out pro-active detection and prevention of ICT problems.
- Service-level management: define, agree and document the required service levels with the users.
- Service continuity management: minimise the impact on ICT service of an environmental disaster.
- Financial management: ensure that the ICT is implemented and managed in a cost effective way.

Technician's Competency Framework

The Technician's Competency Framework developed by Becta is an on-line self-assessment tool, with competency categorised into four different levels (not related to pay). In this way, technicians or school leaders can assess the necessary requirements of the school, the current capability of technical staff, and the additional skills required for increased competency.

Appendix D – Pupils Using Computers at Home

A summary of the implications for a school's Acceptable Use of ICT Systems

ICT is now changing how pupils (and staff) learn and it will soon change what and where they learn. In the UK the percentage of pupils with access to home computers is in excess of 75% and in many Harrow schools is well above 95%.

How well schools capitalise on and support the use of ICT at home through, for example the MLE, will be a key difference between schools. Schools should actively promote the use of ICT to engage with their parents on a range of educational activities. Further guidance can be accessed at Becta's Next Generation Learning site, www.nextgenerationlearning.org.uk.

Main Recommendations for Schools

A school's Senior Management Team should:

- plan a suitable strategy and consult governors;
- consult staff: there are emotive and difficult issues for teachers;
- carry out an audit to determine the level of home ownership and the ICT skills pupils bring with them;
- ensure good access is available, through school or community, for those without ICT at home;
- be persistent in monitoring the use of the school's ICT systems;
- inform parents about the school's approach to safe Internet access;
- examine the possibility of on-line courses for pupils and ensure that parents know about *UK on-line*;
- as soon as possible, be able to accept digital work via an MLE;
- as soon as possible present the issue of e-safety to parents;
- set up a website or give access to the school's MLE that provides parents with advice on the use of home computers;
- establish a basic level of support for ICT use at home to ensure that:
 - all teachers are aware of the issue and know how to respond positively to parents and pupils;
 - there is a willingness for all subjects to accept work produced using ICT at home;
 - assessment criteria are used which recognises work done using home computers;
 - all pupils understand that ICT can be a powerful personal aid and source of information and that if they have access, they should make good use of it, and help their friends as well;
 - parents are provided with common-sense basic guidelines on ways they can help.

Appendix E – Sources of information and guidance about e-safety

For parents, carers and governors:

- Local Libraries;
- Your child's school;
- The National Association of Advisers for Computers in Education (NAACE); a source of advice to the government on Internet and ICT safety: www.naace.org;
- Kidsmart, a practical Internet safety advice website for schools produced by the children's Internet charity Childnet: www.kidsmart.org.uk/;
- The National Children's Homes IT OK site contains several pages of good advice and guidance on safe and acceptable use of the Internet and ICT: www.nch.org.uk/itok/;
- Becta's Internet safety site contains a comprehensive set of advice and guidance for parents and schools: <http://schools.becta.org.uk>;
- The London Grid for Learning (LGfL) has a section developed specifically for parents and carers: <http://cms.lgfl.net/lgfl/web/safety>;
- The very useful Home Office booklet Keep Your Child Safe on the Internet available online: <http://www.thinkuknow.co.uk/parents/>.
- DCSF: National Strategies – Secondary, "Beyond The e-safety Net": <http://nationalstrategies.standards.dcsf.gov.uk/node/173927>.
- Particularly helpful are the resources ('Know IT All for Parents', in 9 languages): www.childnet-int.org/kia at Childnet International;
- Child Exploitation and Online Protection Centre (CEOP): <http://www.ceop.gov.uk/>.

Guidance for school governors

Governing bodies may wish to consider the nomination of a specific governor who has responsibility for ICT in the same way they may have previously appointed literacy and numeracy governors. The ICT governor's responsibilities may include working with the school on the following:

- Considering the funding and training requirements to meet ICT targets (either in pupils achievement or computer to pupil ratios) set by either the school or the national agenda.
- How to respond when offered gifts of free computers.
- Monitoring the performance of the school's technical support provider and how they work in partnership with the school to develop ICT.
- Contribute to the formulation and monitoring of the schools ICT curriculum policy.
- Contribute to the co-ordination of that plan across the curriculum.
- Contribute to the monitoring of the legal requirements for ICT, e.g. legal licensing of software.
- Contribute to the monitoring of the development of ICT as a curriculum subject.
- Monitoring the development and implementation of the school's AUIS Policy; this could include regular monitoring of how pupils and staff adhere to these policies.
- Consider how ICT (particularly the school's MLE) might be developed as a resource for governors.

Where can a school governor go for further help?

Governors might also find the following web sites for school governors to be useful sources of further information: <http://www.governornet.co.uk/> and www.becta.org.uk/start/governors.html.

The National Association of Governors and Managers at: www.nagm.org.uk.

The National Governors Council at: www.ngc.org.uk.

The full text of the document, from which this summary has been adapted, can be found at www.becta.org.uk.

Appendix F – Using New Technology (hints and tips for adults working with young people)

Social Networking hints and tips

Social networking sites provide ways to stay in touch with friends and share photographs, comments or even play online games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the ‘profile’ information you reveal. Be web savvy!

- Social networking sites, such as Facebook, **have a range of privacy settings**. These may be set to ‘expose’ your details to anyone. When ‘open’ anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to “Just Friends” so that your details, photographs, etc., can only be seen by your invited friends.
- Have a neutral picture of yourself as your profile image. Don’t post embarrassing material.
- You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may be bombarded with friendship requests or ‘suggestions’ from people you do not know.
- Choose your social networking friends carefully and ask about their privacy controls. Do not accept ‘friendship requests’ on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example, in Facebook if you write on a friend’s ‘wall’ all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups and networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school project create a new user profile for this.
- If you or a friend are ‘tagged’ in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be ‘friend’ with someone to be tagged in their photo album. If so, you can remove the tag, but not the photo. Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Once something is on the Internet, even if you remove it, the chances are it has already been ‘snapshotted’ by a ‘web crawler’ and it will always be there. Archives of web content are stored on sites like the WayBackMachine.
- Think about your Internet use, adults are just as likely to get hooked on social networking, searching or games. Be aware of addictive behaviour!
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral roles and for as little as £9.99 your personal information can easily be found by a stranger.

Wider Internet hints and tips

- Never tell anyone your password(s) and be careful how you choose them. Most are very predictable. It is easy to find personal details online that might give password clues. You are recommended to include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses, words found in a dictionary, etc.
- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.

- Create yourself a Hotmail (or similar) account when searching for insurance quotes, etc. When finished, either close the email account, or ignore it. Any junk mail generated will then not affect you.
- Be careful when form filling online...., do you know who the data is for? Only answer 'required' questions, do not just give out information because you have been asked for it.
- Never verify banking details online.
- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.
- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.
- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact) do not give out any personal information.
- Popup adverts are often a nuisance. Close them carefully as a 'close' button will often lead you to more advertising as the 'X' might be a graphic.
- If you get an email or popup offer that seems too good to be true it probably is!
- If someone sets things up for you at home, make sure you change your password immediately. Someone with your username and password could impersonate you.
- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you'll need to know the specific URL or user name.
- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing 'adult content' on your computer, the stored cookies may mean you get 'adult pop-ups and adverts'.
- Use legal sites for downloading music, films etc., such as LGfL, iTunes.
- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.
- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as 'net play'. This means that you are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.
- Applications like Skype and iplayer need bandwidth and can slow down the Internet, particularly if you use a 3G mobile stick. Full screen iplayer could use up your allocation and your service may be 'throttled' - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible.
- When you log-into a web site, unless your computer is exclusive to you, don't tick boxes that say 'remember me'.
- Don't leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.
- Don't give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.
- Your school or work laptop (or other equipment) should not be used by friends and family.

If you work with young people:

- Try to provide pupils with direct links embedded into 'pages' in a document, MLE 'room', or interactive whiteboard resource, etc.
- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even innocuous words can bring up adult material.
- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home, you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines.

- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use a YouTube (or any) videos, find out how to embed it using the ‘Source’ rather than a page link, as that exposes pupils to other content.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip, download it (if legal & copyright allows), it might not be there next time.
- If you use your own equipment in school (e.g. cameras or laptops), ensure senior leadership have given permission. Ensure school files (photographs, etc.) are stored in school, not at home.
- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership’s permission, and ensure it is on an encrypted device.
- Video Conferencing – you can be broadcasting without realising it, if you have VC in your classroom make sure it is switched off after use and that the camera is turned away from the class.
- You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don’t just ‘grab stuff’ off the Internet. Use the copyright images from the National Education Network (NEN), LGfL or other sites your school / LA has advised you of. You cannot show DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for ‘adult versions’ of blockbusters.

Email hints and tips

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc. When done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- If you get an email from someone or a company that you have never head of and it asks you to reply to unsubscribe, don’t. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.
- If you get emails that offer you money making schemes (e.g. the ‘Nigerian email’), Russian wives, pharmaceutical products and body part enhancement don’t be upset,. This is spam and junk mail.
- Webmail is useful but insecure, and your email address is easily passed on. Use StaffMail from LGfL.
- If you get spam or junk mail it does not mean that someone has ‘hacked’ into your email; people get email addresses in different ways, it might be a software ‘guess’ – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.
- Only open Email attachments from trusted sources, you won’t get a virus from the initial email text, but it may be contained in an attachment.
- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.
- Don’t give out private email addresses to students and pupils.

Phone hints and tips

- Don’t give out your mobile number or home number to students or pupils.
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the name of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from ‘stranger’ devices within range.

Appendix G – Use of digital and video images

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff needs to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website. Having a website that is easy to maintain and update is helpful and many schools use the WebFronter tool from the London MLE.

Use of still and moving images

Most importantly, take care when using photographs or video footage of pupils on the school website. Consider using group photographs rather than photos of individual children. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

- **If the pupil is named, avoid using their photograph / video footage.**
- **If the photograph /video is used, avoid naming the pupil.**

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film

If showcasing examples of pupils work consider using only their first names, rather than their full names.

Only use images of pupils in suitable dress to reduce the risk of inappropriate use.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images, e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken.

Parental permission should be obtained before publishing any photographs, video footage etc. of pupils on the school website, in a DVD or in any other high profile public printed media. This ensures that parents are aware of the way the image of their child is representing the school; a printed copy of the specific image should be attached to this form. A Parental Permission Form is an appropriate way of achieving this. See the sample permission form on the e-safety portal.

Procedures:

Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by pupils should always be reviewed before publishing it on the school website. Make sure that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that pupils' work doesn't contain any statements that could be deemed defamatory.

Ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

If the school's website contains any guestbook, notice board or blog, they need to be monitored to ensure they do not contain personal details of staff or pupils.

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Digital images – photographs and video clips – can now readily be taken using mobile phones. Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website, e.g. a recent case of a posting on YouTube. It is therefore important to ensure that the risk of inappropriate use is minimised. Are camera/video phones allowed in the school? How is this monitored and enforced? Staff should be advised not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Technical:

Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school.

When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names or in <ALT> tag references when published on the web.

[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]

Many schools are now using video as part of their Visual Literacy work. It is important that staff do not use software to 'rip-out' sections of copyrighted movies without permission.

There are safe online environments for publishing, such as the LGfL portal or Learning Platform and School 'Book Publishing' websites.

Education:

Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Appendix H – Taking encrypted data overseas

(Edited from the 2009 Becta Information Handling Guidance on Data Encryption)

Restrictions on encryption technologies and encrypted devices

Encryption is controlled or restricted in many countries. Many have passed laws, or are considering laws, to maintain law enforcement and national security capabilities through regulation of these technologies.

In some countries, encryption technologies are treated in the same way as weapons or munitions.

Although recommended for protecting data in the UK, some countries ban the use, or severely regulate the import, export or use of, encryption technology. You should always check current restrictions before leaving the UK with encryption software or encrypted data – you can find out about current restrictions from the two websites below. It may be safer to remove the software and data from your laptop or mobile device than to risk violating compliance requirements in these countries. **Not doing so could risk imprisonment or confiscation.** When travelling to countries where encryption is permitted, it is still good practice to store encrypted data on media, laptops or mobile devices in a hotel room safe.

These two general reference sites provide current information on encryption restriction guidance:

- <http://rechten.uvt.nl/koops/cryptolaw/index.htm>
- <http://www.wassenaar.org>

All people that travel as part of an educational visit must ensure they have checked the implications of the above before taking that device abroad.

Countries with encryption import and use restrictions (information correct at August 2008):

- Afghanistan;
- China (import, export and transit controls);
- Hungary (import controls);
- Israel (personal-use exemption – must present the password when requested to prove the encrypted data is personal);
- Morocco (stringent import, export and domestic controls enacted);
- Pakistan;
- Russia (you must apply for a licence);
- Saudi Arabia (encryption is generally banned);
- Tunisia (import of cryptography is restricted);
- Ukraine (stringent import, export and domestic controls).
- China (you must apply for a licence);
- Cuba;
- Ivory Coast;
- Indonesia;
- Iran (strict domestic controls);
- Iraq;
- Liberia;
- Libya;
- North Korea;
- Sudan;
- Syria;
- Vietnam (personal-use exemption for travellers);
- Yemen;
- Zimbabwe.

Take one of the following steps before travelling:

- a) do not take a device with you (*preferred*);
- b) remove any encryption software and encrypted data from your laptop or mobile device (*which will have support implications or breach the UK's own guidelines on information security*); or
- c) apply in well advance for the appropriate licence before leaving the UK.

Embargoed countries (where approval from the UK government is unlikely):

- Burma (you must apply for a licence);
- Belarus (import and export of cryptography is restricted; you must apply for a licence before entry);

Appendix I – Data and MLE Administrator Confidentiality

Possible wording of a ‘contract’ that schools might use to ensure the personal information is treated with appropriate care

When accessing data you must at all times comply with the Data Protection Act. Use of the data must be consistent with the purpose for which the system was constructed. Data must be processed securely and not be subject to any unauthorised use or disclosure.

Staff with responsibility for managing and accessing personal data in the school’s Management Information System (e.g. Capita SIMS) or the MLE (e.g. London MLE: Fronter), or any other systems linked to them, **are strongly advised** to agree to and comply with the following conditions:

1. The data is to be used only for educational purposes and in the interests of the person to whom that data belongs, and not for any other purposes.
2. Personal data is to be shared only with those who need the information to discharge a statutory education function.
3. Only authorised users may access the system and they must never share their login details with anyone.
4. Management of Fronter usernames and passwords is the responsibility of the authorised system manager / Fronter administrator in the school. Where necessary this responsibility may be shared with the authorised system manager in the LA and the system supplier.
5. Care must be taken to protect any data which is printed or otherwise displayed.
6. Procedures should be in place to protect any data in transit. Data must never be taken out of the system in an unencrypted form.
7. Temporary data sets must be deleted as soon as possible.

Harrow's Achievement and Inclusion Service (A&IS) gratefully acknowledges and has referred in this document to the work of:

- British Educational Communications and Technology Agency (Becta);
- Beebug Limited;
- Department for Children Schools and Families (DCSF);
- London Boroughs of Brent and Greenwich;
- *pps-Acit* Computer Consultancy;
- Kent County Council;
- London Grid for Learning (LGfL);
- The London School of Economics and Political Sciences (LSE);
- National Association of Advisers for Computers in Education (NAACE);
- National Association of Headteachers (NAHT);
- The ICT Strategic Group – Harrow Schools and Achievement and Inclusion Service.

**This advice and guidance has been produced by
The Achievement and Inclusion Service of
Harrow Council in collaboration with
Harrow teachers**

28th January 2010

