Annex A

Promoting the Responsible Use of the Internet in Schools

Schools use of the Internet is expanding rapidly and fascinating applications have been developed. Many schools have asked for guidance on ensuring responsible and safe use of this new communications medium.

This leaflet provides an overview of the issues for Headteachers, governors and ICT co-ordinators. A range of approaches is described including education for responsible use and regulation to reduce misuse, leading to advice on writing an Internet Access Policy.

Contents

BCS and NAACE consider that these issues are important and urgent. This leaflet may be copied for educational use without further permission.

Annex A

NAACE

The National Association of Advisers for Computers in Education (NAACE) is the professional association for those who are concerned with inspection, advice, support and development of the use of information and communications technology in education. The Association was established in 1984 and is now a key influential professional association in the field of educational ICT in the UK. NAACE is a Registered Charity and has over 500 members.

The Professional Officer NAACE PO Box 60 Tipton West Midlands DY4 0YS	Telephone: 0870 24 00 480 Fax: 0870 24 00 480 E-mail: prof@naace.org Web site: www.naace.org

BCS

The British Computer Society (BCS) is the leading chartered society in the UK for computing and information systems engineering and is a full nominating body of the Engineering Council. The BCS serves over 37,000 members. The Schools Committee comprises people with knowledge, understanding and experience of ICT in education. It advises the BCS on educational matters and publishes occasional papers.

The BCS Schools Committee British Computer Society 1 Sanford Street Swindon SN1 1HJ	Telephone: 01793 417417 Fax: 01793 480270 E-mail: bcs@hq.bcs.org.uk Web site: www.bcs.org.uk/

ISBN **1-902505-15-8**

Web: The latest version of this document will be maintained on the Web: http://www.bcs.org.uk/iap.html

Authors: Steve Bacon
Peter Banbury
Sandra Crapper

Acknowledgements:

We would like to thank members of NAACE, the BCS and other organisations who have read and commented on draft copies of this leaflet and Kent County Council for permission to copy the Acceptable Internet Use Statement and the Rules for Responsible Internet Use.

Annex A

Promoting the Responsible Use of the Internet in Schools

Introduction

For the past twenty years or more, schools have been developing their use of information and communications technology (ICT) with the aim of raising the quality of education and enhancing learning opportunities for young people. Great strides have been made in a relatively short space of time and the advanced computer systems now to be found in schools bear little resemblance to the simple computers with which schools started in the early 1980s. Increasing computer power and sophisticated software have brought immense benefits to the classroom across the curriculum and have provided young people with new and exciting learning opportunities.

More recently, the advent of easy access to electronic communications has brought a new dimension to the use of ICT in schools. Through the Internet, schools and their pupils have access to a global network of information resources. These not only enhance their access to resource materials but also provide opportunities for world-wide communication with other pupils and teachers, provide access to cultural, social and leisure information and provide schools with a range of support services.

Extensive use of ICT in schools raises organisational and management problems; there is also the potential for misuse of the technology. In recent years this has included pupils gaining unauthorised access to computer files, the irresponsible deletion of pupils' work on school networks, the exchange of discs containing pornographic images and so on. The Internet also presents schools with organisational and management problems, and extends the scope for misuse. However, there are educational, management and technical solutions which can help to minimise the risk of the inappropriate use of the Internet. The aim of this document is to help schools by describing some of the problems and outlining possible strategies for their solution.

Schools will need to bear in mind that their pupils will be likely to access the Internet in a wide range of contexts both within, and outside school. Apart from using the Internet to support learning in the traditional school classroom, pupils will benefit from opportunities to access the Internet in after-school and homework clubs, in youth clubs, public libraries and other community services, in Internet cafés and shops, and at home. Additionally, the Government's intention that at least 50% of pupils should have their own e-mail address by 2002 and the general acquisition of e-mail addresses by their parents will make e-mail as common as the telephone. It will not be long before there is almost universal access to e-mail and the Internet. As a result, pupils' use of the Internet may be greater at home than in school. It therefore becomes very important for schools not only to police their own provision but also to develop in their pupils' well-understood and responsible attitudes to the Internet. They need to be able to make responsible decisions for themselves, not just adhere to a set of rules imposed by others.

This document has been written for all schools although it is recognised that the issues for schools in the primary sector are likely to be different from those in secondary or special schools. Each school will need to decide what measures it needs to take to prevent inappropriate use of the Internet in their establishment and to develop responsible use of the technology by young people.

Annex A

1: What is the Problem?

a. The Internet System Itself

It is wrong to think of the Internet as a coherent system; it is simply a very large number of individual or networks of computers any of which may be linked electronically to any other. Some of the computers that can be accessed on the Internet belong to large organisations while others are desktop computers owned by individuals. Although these computers are scattered around the world, modern worldwide communications technology means that they are all equally easily accessible.

The Internet is anarchic. There is no overall control and there is no censorship. It is up to individual information providers what views they will express and how they will express them, what text they will make available for others to read, and what images, video and sound they will provide.

The Internet is dynamic. Individual information providers can change their material overnight so you can never be sure that what you saw yesterday is still the same today – or is even there at all! New information providers join the system on a daily basis and others disappear; it is not easy to keep up to date with the huge number of sources of information.

b. The Internet Structures

The Internet is accessed through a number of different structures, all of which give rise to potential problems when used by young people.

The **World Wide Web** (WWW) makes information easily available to the user. Pages of information (collected together as *Web Sites*) are presented in an attractive format containing text, images, sound, animations and video. The user moves from one page to another by clicking on buttons or text prompts on the screen. Often the process takes the user from one information provider to another in an apparently seamless manner. It is easy for the user to 'browse' the system (*surfing the net)*, but it is also easy to get lost, or to be distracted from the task in hand by following up other apparently interesting or intriguing links. Some of these links may be to material unrelated to the original purpose of the use of the WWW, and some material may be unsuitable for young people. While the WWW offers a treasury of material for children to use, and access is very easy, it also means that less suitable material is easily accessible or may be viewed accidentally.

Internet **Newsgroups** allow users around the world to share in discussion on a wide variety of topics. There are currently over 30,000 such discussion groups, only a few of which are likely to be of interest in an educational context. By accessing one of the groups, the user can read messages on a particular topic, which have been placed (*posted)* by others. In order to participate in the discussion, users can post their own replies. Newsgroups do not depend on people being connected to the Internet simultaneously. The user connects to the Newsgroup of their choice, reads recent messages, posts their replies and then disconnects. Although Newsgroups can be an effective way of sharing ideas and information, they may also encourage discussion of topics that may be inappropriate for young people. In some cases, the information provided is either factually incorrect, represents biased or extreme personal opinion or is designed to be misleading or corruptive. Newsgroups not only allow text to be shared; it is also possible for images, sounds and video clips to be posted for others to access and some Newsgroups are used explicitly for this purpose. There is no central censorship of Newsgroups, although some are censored or *moderated*.

Internet **Chatrooms** are similar in concept to Newsgroups but depend upon several people contributing simultaneously. In these areas, usually accessed via pages on the WWW, several users can read and post contributions concurrently. Users often find the casual Chat activity slow, frustrating and, when it is not focused on a clear educational objective, a considerable time waster. It can also be expensive since the user has to be connected to the Internet for the duration of the Chat. As with Newsgroups, most Chatrooms are not censored. Because of the anonymous nature of the communication, concern has been expressed about the possibility of Chatrooms being used to exert undue influence over young people.

Electronic mail (e-mail) is an extremely powerful communication tool. Internet users can send e-mail to anyone whose e-mail address they know. Young people will benefit considerably from being able to communicate easily with other people around the world. Not only will they make contact on a social basis, but they may also be able to make contact with other adults and young people in connection with their studies. The opportunity to contact other people in different social or geographical contexts is particularly powerful. Of course, pupils may also engage in less appropriate communications, and be vulnerable to receiving unsolicited and inappropriate communications from other people. To provide some protection in this respect, some e-mail systems are being designed to enable the user to specify only those people from whom they are willing to receive e-mail.

Increasingly, schools and pupils will have their own **Web Sites**. This facility is offered by most Internet service providers free of charge, or at very low cost, or may be provided by the school within its own network. A school will need to take steps to ensure that its own web site does not contain inappropriate material. Where the school is offering space for individual pupils to manage their own Web Sites there will need to be checks on the content to ensure appropriate use. Where the student is managing their own Web Site on another system the school will have no direct control but may wish to offer advice on good practice and responsible use.

All the above structures exist within the overall concept of the Internet. Individual computer users may also allow external access to their computer via what are known as **Bulletin Boards**. These usually exist outside the Internet and are often run by individuals rather than organisations. They are services where the user can dial up directly, access information, post questions and read other people's comments and answers. Most are accessed via their own telephone number rather than via the telephone number of an Internet service provider. Contacting such a Bulletin Board will be charged at the price of a direct telephone call to that locality. Thus, the use of some Bulletin Boards can be very expensive. Schools which purchase access to a single Internet service provider and have their system pre-set to dial only that provider (for example, through an ISDN telephone line) will not be able to access Bulletin Boards and hence are not likely to have a problem with access to unauthorised phone numbers. However, schools using a simple modem where the phone number to be dialled can be easily changed are more vulnerable in this respect.

c. The Internet Content

Within the range of services available on the Internet there is very wide variety of content. Although every conceivable topic or area of interest is to be found somewhere on the Internet, the material available varies hugely in quality. Some of it is heavily biased reflecting the opinions of those who prepared it. Some of the material is inaccurate or misleading often due to the ineptitude or lack of experience and knowledge of the originator; in some cases the originator is intending to mislead for a variety of reasons.

Pupils using the Internet need to be aware of the issues of quality and veracity, exercising caution and judgement in their use of any material they find.

There is a considerable amount of pornographic material including text, sound, pictures and video to be found on the Internet. There are Web Sites, Newsgroups and Bulletin Boards dedicated to carrying such material. However, the problem is confounded because some Web Sites of an apparently harmless nature may include some pages with explicit content. Other areas of concern to schools include the availability of information on the Internet relating to the misuse of drugs and the promotion of violence, intolerance, racism and extreme political and social views.

Finally, standards of what is appropriate content for worldwide publication will inevitably vary from one person to another. Standards of expression, language and tone will vary. People will differ in their views about what are acceptable text and images for publication. Cultural and social differences will mean that what is acceptable for one person, may not necessarily be acceptable for another.

Schools should also bear in mind that the vast majority of the content of the Internet is written by and for adults. This means that the reading level may be too difficult for some children, the language used may be inappropriate or the ideas expressed inappropriate for the maturity of the reader.

d. The Legal Context

There is no legal definition of the term 'pornography' and there are few legal precedents relating to the use of the Internet. There are a number of laws which are likely to apply to the use of the Internet in certain circumstances including the Obscenity Acts of 1959 and 1964, The Protection of Children Act 1978, The Indecent Displays Act 1981 and The Criminal Justice Act 1988. The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990. In many cases, laws relating to copyright, libel, obscenity or incitement to racial hatred are likely to apply to the use of the Internet.

While the legal position is not always well defined, schools should bear in mind that there is a legal framework that could be applied to Internet use.

e. The Ethical Context

While schools will be properly concerned about the legality of Internet use and ensuring that neither they nor their pupils are liable to prosecution, it will, perhaps, be more important for them to recognise their overall moral responsibility and their duty to provide protection for the pupils in their care. Parents will expect schools to promote high standards in relation to the use of computers and the Internet whether or not the material being accessed is necessarily illegal. They will expect schools to develop the same levels of responsibility in pupils in this area as in any other. Recognising its importance, many schools already address this issue in their personal and social education programme. By whatever means, schools should be able to demonstrate that they have taken all reasonable precautions with regard to Internet access and have strategies to promote responsible use both within and outside the school.

The possibility of inappropriate use of the Internet by pupils is something that needs to be well understood by teachers and other staff, all of whom may come into contact with the problem. Teachers may be faced with accidental access to inappropriate material during the course of a lesson, or may encounter pupils who are explicitly searching for such material. It is part of the school's responsibility to its staff to ensure that they are never

placed in a situation for which they are not prepared and where they are unaware of the school's policies.

2: Strategies for Consideration

Schools must be made safe places in which pupils learn to take a full part in society and learn to handle the risks and responsibilities inherent in adult life. Teachers and managers need to create the right balance between protecting pupils, securing IT systems and improving access to systems and the Internet.

All parts of society have called for improved solutions and the press has frequently highlighted the political and social issues involved. While the main areas of concern are understood, the development of effective solutions will take time.

This section outlines strategies in three areas - educational, management and technical. Schools will need to take a holistic approach in order to resolve the complex and wide-ranging issues involved.

a. Educational Strategies

There are two main approaches to Internet access, education and regulation. Pupils may be educated to develop a responsible attitude to computer and Internet use within and outside the school environment in the expectation that pupils will make the right decisions if they understand the issues. The school will also need to regulate Internet access. Primary pupils cannot be relied upon to foresee every possible danger. Faced with suspect material, even the most responsible children may not have the experience or maturity to make informed judgements. For infants and some juniors, Internet access is likely to be directly controlled by an adult working with a small group of pupils. A rules approach may be taken with older primary and secondary pupils, whereby a code of conduct is agreed or set. Both types of approach, education and regulation, may be appropriate depending on age and maturity of the pupils. Each school will need to strike the right balance in writing its Internet access policy.

Pupils' use of the Internet may be greater at home than in school, and we may need to extend the educational approach to include parents. Families may need to be helped to develop strategies to cope with the knowledge and influences introduced by the Internet and to understand the consequences for their lives.

The Internet makes available an even wider range of material than CD-ROM, TV and video although many pupils still simply copy entire articles and images uncritically. Pupils' information handling skills in selection and in checking origin, currency and accuracy have become vital. Maturity in the application of this information will result from improved knowledge and awareness of the Internet.

There are responsibilities for the use of ideas and materials owned by others. Plagiarism is almost encouraged by the availability of coursework on-line, or should this be regarded as the provision of good exemplar material? The issue of copyright needs to be discussed and pupils encouraged to acknowledge sources.

Teachers will need to investigate the nature of the different media and the difficulties that pupils may experience with retrieval and in dealing with large quantities of information. Well-defined tasks with lists of suitable sources will direct investigations and help ensure success. Open-ended research involving the unstructured use of search engines or catalogues should be restricted to pupils that have the necessary information handling skills.

Staff awareness of the issues and understanding of the school's strategies is important. Time will be required for teachers to integrate ICT into the curriculum and revise study skills teaching. Teachers' own skills may need to be developed and home access to ICT and particularly the Internet is to be encouraged. Many advisers and other groups have thought through these issues in detail and could be used to raise staff awareness and to share the experience of other schools.

Pupils should never feel uncomfortable or threatened by messages received or material seen. As with bullying, the natural approach should be to tell a teacher. An integrated policy covering all such areas will need to be developed. Pupils may have to decide for themselves what material is appropriate and may need help in making such decisions.
The personal, social and health education (PSHE) programme would be an appropriate context to discuss the responsible use of media including video, computer games and the Internet.

While schools give pupils structured access to the e-mail and the Web, at home the same pupils may have open access. The school may wish to work in partnership with parents to raise awareness and resolve such issues.

b. Management Strategies

Within the curriculum planning process, management will review the contribution made by Internet use to teaching and learning. Schools will wish to ensure that they have done everything reasonably possible to ensure appropriate and safe use of the Internet. A key strategy is to write an Internet Access Policy, which is covered later.

IT systems are expensive and becoming critical to efficient curriculum delivery and to school administration. To reduce any misuse of computer facilities, senior management will need to allocate resources for the implementation of technical strategies and ensure they are effective. ICT use has increased rapidly as interest in resources such as the Internet has exploded. This can result in IT systems becoming overloaded, unless the increase in use is managed and matched by investment in storage and capacity.

By setting the criteria for use and access, staff and pupils will be reminded that the school’s IT system has been installed to enhance and extend pupils' education. One regulatory mechanism is to maintain a register of users, or a list of pupils whose access has been removed.

To protect the school and encourage appropriate use, staff and older pupils may be asked to sign acceptable use statements. A number of LEAs are recommending that schools obtain guardian's agreement to pupils' use of the Internet. Once rules for the responsible use of the Internet have been agreed they can be displayed near computers and copies given to pupils and parents.

The school will need to take a view on the degree of pupil autonomy in Internet access and the balance between privacy and control. The approach to supervision of Internet access will vary according to age. At Key Stage 1, an adult may access e-mail or the Web for the class or group, while pupils from 8 to 16 years may be supervised less directly and sixth form students given open access. Supervision strategies will need to be devised and implemented. IT systems available for private study in a library or resource centre could be positioned in clear public view to encourage a responsible approach to Internet access.

Wherever pupils interact with the public by telephone, e-mail or web site, particular care is required to ensure the communication is appropriate. Pupils need to follow sensible rules for personal safety, for instance never giving full name, a home address or telephone number. Appropriate use may take time to develop.

The school will wish to control the quality and presentation of material on its Web site. Although printing names with photographs is common practice in local newspapers, many schools do not publish photographs with pupils' names on their Web site.

With the rapid increase in Internet access, management will need to revisit its policy and practices on a regular basis. Advice may be sought from the sources given in the references section, the LEA and your IT systems suppliers.

c. Technical Strategies

Technical solutions to social issues cannot be expected to be fully effective by themselves, but they should form an important part of a holistic approach.

IT systems must be designed to withstand attack including virus corruption and hacking as well as accidental damage by users. Pupils' access to the Internet presents particular risks as it includes use of both internal and external systems. Standard good practice in network security becomes ever more important. The design and configuration of the school's IT systems may need to be reviewed by a team chaired by a senior manager, which includes the IT co-ordinator and systems manager, assisted by LEA staff.

Restricting access to inappropriate material is often the first issue to be tackled. Four overlapping approaches have evolved. These can be referred to as blocking, approved lists, filtering and rating, although these categories are often confused.

1. A blocking strategy generally removes access to a list of unsuitable sites or newsgroups. Maintenance of the list is a major task as it may contain thousands of sites, and changes must be made frequently.
2. An alternative strategy is to permit access only to approved sites - the *walled garden* approach, but it is difficult to predict the breadth of pupils' questions.
3. Filtering examines the content of Web pages or e-mail messages for unsuitable words. The advantage is that no prior work is required, but there are problems, for instance with a Web page containing images only. Filtering of Web searches reduces pupils' opportunities to locate unsuitable material.
4. Rating systems give each Web page a rating for sexual content, profanity, violence and other unacceptable content. Web browsers can be set to reject any pages not rated appropriately for the pupil. At present few pages have been rated and, without a consistent international approach, rating is unlikely to become a viable strategy.

As new sites appear every day, none of these systems can be completely foolproof and a combination of approaches will be required. It may be important to establish who decides what is appropriate and whether the criteria used suit the pupils in your school. Another question is whether the system covers an adequate range of languages.

Blocking and/or filtering may be performed by the Internet service provider (ISP), by the LEA where a wide area network is used, or at school level. Wherever performed, sufficient resource should be allocated to ensure that the system is effective and clear guidelines provided to ensure the protection is appropriate to the various client groups. In due course, it will be possible to alter the degree of control to suit the age and learning context of the pupil, however this could require a great deal of local management.

E-mail presents particular dangers due to the large volume of messages and the ease of communicating into and out of a safe area such as a school. Software to restrict addressees to a set list might be appropriate, and the filtering of e-mail for unsuitable content is possible.

In order to protect pupils and help the school to demonstrate that ICT systems are being used responsibly, occasional monitoring of files or the sites visited will be necessary. Senior management may wish specifically to sanction any monitoring and will wish to let pupils know that monitoring is taking place. Software is available that can monitor continuously every site visited. While such strategies could help assure management that access is reasonable, it brings additional expense and will require time to manage.

There is a fine line between intensive but appropriate use of the Internet and inappropriate use such as downloading large files for leisure purposes. This theft of system resources can be limited by storage and time quotas and by monitoring use.

3: Writing a School Internet Access Policy

Introduction

It is possible to obtain a ready-made Internet Access Policy for your school from a number of sources, including the Internet itself. However, it is advisable that each school sets aside time to develop its own policy. This will ensure that members of staff have the opportunity to talk through some of the issues surrounding the Internet in education, and that the policy reflects the local situation.
The outline policy below takes the approach of raising questions for schools to consider in the writing of their own Internet Access Policies.

Background

The Internet is a valuable resource that can raise educational standards by offering both pupils and teachers opportunities to search for information from a very wide range of sources based throughout the world. As with any school resource, ICT needs to be organised and managed to maximise its effectiveness and the contribution it can make to developing and supporting the educational policies of the school. Every school should develop an overall ICT Policy and a statement on the use of the Internet should be part of that policy.

Some of the information to be found on the Internet may be inappropriate for pupils, and it is wise to have a policy in place that takes this into account. Management has a duty to ensure that before using the Internet with pupils, staff has had the opportunity to discuss how they will deal sensitively with inappropriate use. The policy will help to define appropriate and acceptable use by both staff and pupils and offer a focus for continual debate. An effective policy is one to which staff and pupils have agreed.

The DfES has specified that a policy to prevent pupils accessing unsuitable materials is a requirement of funding from the National Grid for Learning Standards Fund.

An Outline Policy on the Responsible Use of the Internet

As with all policies, Governors and teachers need to be involved from the start. It may be that your school already has a Policies Working Group, or a member of staff that works closely with the governing body to develop and monitor school policies. An Internet access policy should build on these existing structures, and will need to involve the ICT Coordinator.

a. The Internet in School

How will the use of the Internet enhance pupils' educational opportunities?

How will NGfL resources be used to raise educational standards?

How will effective use of the wealth of material on the Internet be monitored?

What benefits will Internet use bring to the professional work of school staff?

How will ICT improve the school's management information systems?

Will the school use the Internet as a channel of communication to government, LEA, other educational establishments?

How does the school see the relationship with the community changing with improved access to communications?

b. The Internet in the Curriculum

How will Internet access be integrated into learning activities?

Who will be responsible for developing pupil and staff research skills including the effective, reasonable and legal use of information retrieved?

Which subject(s) will focus on developing pupils' information handling skills?

Will the school establish its own web site?

Will pupils' work be published on a school or any other website?

How will the school make use of e-mail facilities?

How will pupils be educated to validate information and messages communicated over the Internet?

How will children be educated to follow sensible rules for personal safety?

c. Responsibility

How will pupils be educated to take responsibility for Internet access?

How will pupils be made aware of the issues of unacceptable use?

How will intellectual property rights and copyright be discussed?

How will children report if they feel uncomfortable about material or messages?

What action will teachers take if pupils report receipt of unacceptable material?

How will parents be kept informed of the school's strategy?

Will a guardian's permission be sought before pupils are allowed Internet access?

Will the school work with parents to encourage appropriate use outside school?

Will staff and pupils be asked to sign acceptable use statements?

d. Internet Access

Who will use the equipment and where will it be located, e.g. public area?

Which age groups of pupils will be supervised, and in what way?

How will you identify and register authorised users?

Will there be restrictions on use of equipment?

Which Internet Service Provider will be used, e.g. LEA, commercial provider?

Does the school's ISP provide a filtering system appropriate to the age of pupils?

Will the school implement any filtering additional to that provided by the ISP?

Who will be responsible for password security?

e. Monitoring

How will the school evaluate the effectiveness of ICT use?

How often will the ICT system in the school be checked for inappropriate material and virus checking?

How will pupils be informed that checks are made on files held on the system?

Can the school work with the ISP to review and improve the filtering system?

Will regular reports on use be submitted to Governors?

f. Sanctions

What are the school's procedures for dealing with pupils who access unsuitable materials?

g. Dissemination and Review

How will staff and pupils be made aware of the policy and its content?

Who will be responsible for keeping this policy up to date?

How often will it be reviewed?

4: Resources and References

Organisations that provide useful information relating to establishing an Internet Access Policy

Association of Co-ordinators and Teachers of IT (ACITT)
www.rmplc.co.uk/eduweb/sites/acitt/aup.html

Acceptable use policy for the Internet in UK Schools
BECTa
www.becta.org.uk

Advice and guidance on computer misuse
British Computer Society
www.bcs.org.uk/news/misuse.htm

A guide for schools prepared by the BCS Schools Committee
Cambridgeshire County Council
http://edweb.camcnty.gov.uk/ngfl/
Advice to Cambridgeshire schools on Internet access
Connecticut, USA
www.groton.k12.ct.us/mts/mtspol1.htm

Groton District Internet policy for their public school system
DfES Virtual Teacher Centre
www.vtc.ngfl.gov.uk/vtc/schoolman/policies.html

Government information on developing policies for ICT usage in schools
Internet Watch Foundation
www.internetwatch.org.uk

Annex A

This site invites people to report inappropriate web sites they come across. Funded by DTI Ireland – National Centre for Technology in Education
http://www.ncte.ie/support.htm

A comprehensive advice sheet on Internet safety
Kent County Council
www.kent.gov.uk/ngfl/policy.html

Comprehensive information on implementing an Internet Access Policy
National Union of Teachers (NUT)
www.teachers.org.uk/keypol/kp_ict.html

NUT policy on the developing use of ICT in schools
National Action for Children (NCH)
www.nchafc.org.uk/internet/index.html

Guides on Internet usage
Parents Information Network (PIN)
www.pin-parents.com

An introduction to the Internet – comprehensive guidelines on using the Internet safely
Recreational Software Advisory Council on the Internet (RSACi)
www.rsac.org/fra_content.asp

Promotes the use of a rating system for web sites, and acts as a third party rating bureaux
Staffordshire Learning Net
http://www.sln.org.uk/doc2.htm

A computer security policy including Internet access, with sample materials
Yolo County, USA
www.yolo.k12.ca.us/policy1.htm
Example of Yolo County's acceptable use policy

Annex B1

Lancashire County Council - ICT Security Policy for Schools

Implementation Programme

Schools will need to adopt an ICT Security policy that consists of:

Whole school

- ICT Security policy for schools – adopt LEA 'model' **ICT Security policy** or create own policy. (Essential)
- Governing Body and Headteacher to implement procedural aspects of policy - follow requirements detailed in LEA 'model' policy in **Annex B2**. (Essential)
- Backup strategy – recommended strategy included in LEA 'model' policy as **Annex B3**. (Advisable)
- Hardware inventory – recommended proforma included in LEA 'model' policy as **Annex B4**. (Essential)
- Software inventory – recommended proforma included in LEA 'model' policy as **Annex B5**. (Essential))
- Security guidelines – minimum recommendations included in LEA 'model' policy as **Annex B7**. (Advisable)

For Staff

- E-mail and Internet Use policy – recommended policy included in LEA 'model' policy as **Annex A**. (Essential)
- Rules for ICT Users – recommended rules included in LEA 'model' policy as **Annex C1**. (Essential)
- E-mail and Internet use good practice statement – recommended statement included in LEA 'model' policy in **Annex C1**. (Essential)
- Staff declaration form – recommended form included in LEA 'model' policy in **Annex C1**. (Essential)

For Students

- E-mail and Internet Use policy – recommended policy included in LEA 'model' policy as **Annex A**. (Essential)
- E-mail and Internet use good practice - Rules for ICT Users statement - recommended statement included in LEA 'model' policy in **Annex C2.** (Essential)
- Pupil / Parent consent form - recommended form included in LEA 'model' policy in **Annex C2**. (Essential)

For Third Parties

- E-mail and Internet Use policy – recommended policy included in LEA 'model' policy as **Annex A**. (Essential)
- E-mail and Internet use good practice - Rules for ICT Users statement - recommended statement included in LEA 'model' policy in **Annex C3**. (Essential)
- Third party consent form - recommended form included in LEA 'model' policy in **Annex C3**. (Essential)

Note: To ensure that the signature form is on the same piece of paper as the rules being agreed to, Schools may wish to print the appropriate Rules and Consent form side by side in A5 format on an A4 page.

Annex B1

Each of these documents will need to be reviewed on a regular basis. Completing the following table will document the policies adopted by the school and assist in identifying the relevant review process. Any other implementation issues can also be documented in the following section.

Documents relating to ICT Security Policy for Schools

Document Name	Model document used or Schools own version?	Location of Document	Produced / Reviewed By	Last Review Date	Date next Review is due
ICT Security Policy	**Model used.**	**File in staff room cupboard/ server**	**MB**	**DEC 13**	**DEC 14**
E-mail & Internet Use Policy (Annex A)	**Model used**	**File in staff room cupboard/ server**	**MB**	**DEC 13**	**DEC 14**
Procedural Aspects (Annex B2)	**Model used**	**File in staff room cupboard/ server**	**MB/MC.**	**DEC 13**	**DEC 14**
Backup Strategy (Annex B3)	**Own used**	**File in staff room cupboard/ server**	**MC**	**DEC 13**	**DEC 14**
Hardware Inventory (Annex B4)	**Model used**	**File in staff room cupboard/ server**	**MC.**	**DEC 13**	**DEC 14**
Software Inventory (Annex B5)	**Model amended & school software toolkit included.**	**File in staff room cupboard/ server**	**MC.**	**DEC 13**	**DEC 14**
Security Guidelines (Annex B6)	**Model amended**	**File in head teachers office/server**		**DEC 13**	**DEC 14**
Rules for ICT Users – Staff (Annex C1)	**Own models used.**	**File in head teachers office/server**	**MB/ALL STAFF**	**DEC 13**	**DEC 14**
Email & Internet Use Good Practice for Staff (Annex C1)	**Own models used.**	**File in head teachers office/server**	**MB/ALL STAFF**	**DEC 13**	**DEC 14**
Declaration form for Staff (Annex C1)	**Own models used.**	**File in head teachers office/server**	**MB/ALL STAFF**	**DEC 13**	**DEC 14**
Email & Internet Use Good Practice – Rules for ICT Users for Students (Annex C2)	**Own models used.**	**File in head teachers office/server**	**MB/ALL STAFF**	**DEC 13**	**DEC 14**
Pupil / Parent Consent Form (Annex C2)	**Own models used.**	**File in head teachers office/server**	**MB/ALL STAFF**	**DEC 13**	**DEC 14**

Nominated System Manager:	**Marie Baxendale**

St. Joseph's Catholic Primary school Information Access and Security Policy *December 2013*

Text identified by the use of italics and bold underlining can be replaced by the schools' own text as applicable

Purpose

This information access and security policy provides clear direction and support for information security that is applicable to all staff at all levels of the organisation. The policy describes the means by which the school aims to preserve confidentiality, integrity and availability of data.

Confidentiality:	information is accessible only to those authorised to have access
Integrity:	safeguarding the accuracy and completeness of information
Availability:	ensuring that authorised users have access to information when required

It is acknowledged that the school has legal, statutory and contractual requirements with which it must comply. The school complies with the rules of good information handling, known as the data protection principles and the other requirements of the Data Protection Act.

The senior manager in the school is invested with overall responsibility for information security is - MRS. MARIE BAXENDALE-HEADTEACHER.

This policy will be reviewed and updated every **DECEMBER** the next date being **DECEMBER 2014.**

Specialist security advice will be sought where necessary. The **LA** will be consulted as a source of such advice, for example for data protection or network security issues.

Organisational Security

Allocation of responsibilities – Information and asset classification and control. An accurate inventory is maintained of all the assets associated with information systems.

This is the responsibility of MRS. MARIE BAXENDALE- HEADTEACHER.

Each 'information asset' (e.g. information system, database, etc) has an owner who is responsible for its day to day security. Information is classified according to its degree of sensitivity and confidentiality, indicating the need and priority for its protection and is labelled appropriately (e.g. level 1 is all staff access, level 5 is Headteacher only). Each classification has defined procedures for copying, storage, transmission (e.g. post, fax, e-mail, telephone) and destruction.

Information	Databases, documentation, manuals, plans, archived information
Software	Application and system software
Physical	Computer and communications equipment
Services	Power, air conditioning

Authorisation level	Names of key personnel	Authorised to:
1. MANAGER	MRS.M.BAXENDALE	AUTHORISE ORDERS
2. OFFICE	MRS.L.CURTIS	RAISE ORDERS/ PROCESS INVOICES.
3. CLERICAL	MRS.A.BULLEN	" " " " " "

Information Asset	Purpose	Sensitivity Level	Keeper	Authorisation Level
PRIVATE FUND	SCHOOL FUND	1	OFFICE	3
SIMS FINANCE	FINANCE	1	OFFICE	
SIMS.NET	INFORMATION	1	OFFICE	

Software and Physical and Services Assets	Purpose	Keeper
EQUIPMENT REGISTER	ASSET REGISTER	MRS.M.BAXENDALE

It is acceptable to include here a SIMS printout which covers some or all of the aspects above.

Personnel Security

This is the overall responsibility of **MRS. MARIE BAXENDALE-HEADTEACHER.**

Security in job responsibilities

Security responsibilities are clearly documented and where appropriate, addressed at the recruitment phase and included in contracts of employment. Personnel screening processes for permanent and temporary staff includes appropriate controls (e.g. availability of satisfactory references, confirmation of claimed academic and professional qualifications, independent identity checks). Staff sign a confidentiality or non-disclosure agreement as part of their initial terms and conditions of employment. (*Sample appended*). There is a formal disciplinary process for employees who violate security policies and procedures and employees are made aware of the action to be taken if they disregard security requirements.

Information security education and training

All staff receive appropriate training and regular updates in security policies and procedures before access to systems is granted. (Sample training programme appended). This includes training in security requirements, controls and legal requirements, as well as in the correct use of information systems. (E.g. Log-on procedures).

Responding to security incidents and malfunctions

A formal procedure exists for reporting and responding to security incidents, malfunctions and weaknesses. (Procedure appended). All staff are aware of their responsibilities to note and report such incidents through the proper management channels as quickly as possible. Recovery is carried out only by appropriately trained and experienced staff. Users are made aware that they

should not, under any circumstances; attempt to prove a suspected security weakness as this could be interpreted as potential misuse of the system.

Physical and environmental security

This is the overall responsibility of **MRS. MARIE BAXENDALE-HEADTEACHER.**

Secure areas

Areas in which critical or sensitive information is processed are physically secured to prevent unauthorised access, damage or interference. Control is achieved by conventional security procedures (e.g. doors and windows locked when unattended, external protection for ground floor windows, intruder detection systems). Access to secure areas (if applicable) is controlled and restricted to authorised personnel only, with authentication procedures (e.g. swipe card, pin number).

Equipment security

Equipment is sited or protected to minimise the risk of theft (including security marking), damage (e.g. fire, water, and impact), and power failure (e.g. uninterruptible power supply or UPS). Cabling is protected from interception or damage (e.g. use of conduit, fibre, avoidance of public areas, routed underground, away from communications cables). Equipment is correctly maintained and serviced by authorised personnel. (*Names could be inserted here such as Westfield Centre*).

Off-site security

Equipment is not taken off-site without authorisation. Where necessary and appropriate, equipment is logged out and back by (*Insert name here*). Equipment and media taken off the premises is not left unattended in public places. Portable computers are carried as hand luggage and disguised if possible when travelling. Home working is subject to suitable controls.

Secure disposal or re-use of equipment

Appropriate arrangements are made for the secure disposal of media containing sensitive information. Confidential paper documents are securely disposed of (e.g. by shredding, incineration). Storage devices containing sensitive information are destroyed or securely overwritten (rather than using the standard delete function) prior to disposal. Equipment containing storage media (e.g. hard disks) is checked to ensure that sensitive data and licensed software have been removed or overwritten prior to disposal or re-use.

Clear desk and screen policy

Paper and computer media are stored in suitable locked cabinets were appropriate. Sensitive printed material is cleared from printers *immediately and shredded/disposed of by…***ADMIN STAFF/ TA'S** Business critical information is held in a fire resistant safe or cabinet, with **BACK-UP COPIES BEING TAKEN HOME EACH NIGHT BY ALTERNATE MEMBERS OF THE ADMIN STAFF.** PCs and printers are not left logged on when unattended and are protected as appropriate by key locks, passwords or other controls when not in use. Users terminate active sessions and log off when out facility is afforded by password protected screen savers.

Annex B1

Communications and operations management

This is the overall responsibility of **MRS. MARIE BAXENDALE - HEADTEACHER.**
Operating procedures are documented and maintained. *Local information should be stored here.* Changes to systems are controlled with significant changes identified and recorded, following assessment of the potential impact

of the change and the change details communicated to the relevant persons. Incident management procedures are in place to ensure a quick, orderly and effective response to security incidents.

Protection against malicious software (viruses, etc.)

Software licensing requirements are compiled with and the use of unauthorised software is prohibited. Anti-virus detection and repair software is installed and regularly updated. Electronic mail attachments, downloads and any files of uncertain origin on electronic media or downloaded are checked for malicious software before use. Appropriate business continuity plans for recovery from attack are in place (e.g. data and software back-up and recovery arrangements). *Local information is required here.*

Housekeeping and network management

Back-up copies of essential information and software are taken regularly according to an appropriate schedule. At least three generations of back-up information are retained for important applications and are stored with an appropriate level of physical protection at a sufficient distance to escape a disaster at the main site. Back-up media and restoration processes are regularly checked to ensure that they are effective. Controls are in place to ensure the security of data in networks and the protection of connected services from unauthorised access.

Back-up procedure - data	Routine	Responsibility
Fresh tape in machine each day.	Each morning take out previous nights back-up from machine & securely store ready for transportation to admin staff.	Mrs. L.Curtis / Mrs. A. Bullen – alternatively.
4 tapes are used on Fridays.		
The last tape used is taken home, the days before is kept in the safe.		

Electronic mail

Guidelines exist on when to use and not to use e-mail. Staff understand the potential difficulties of the difference between electronic and traditional forms of communication (e.g. speed, message structure, degree of informality and vulnerability to unauthorised actions and attack – interception and viruses). Staff understand their responsibility not to use e-mail in such a way as to compromise the good name of the school (e.g. defamatory e-mail, harassment, unauthorised purchasing). *Staff guidance appended*.

Access control

This is the responsibility of **MRS. MARIE BAXENDALE HEADTEACHER.**

User registration

Formal procedures are in place to control the allocation of access rights to information systems and services. Users have authorisation from the system owner and the level of access is appropriate for the purpose. User access rights are regularly reviewed; access rights of leavers are removed immediately and redundant users IDs removed. Privileges associated with each system and user are identified, allocated on a need-to-use basis and kept to a minimum.

User password management

Users understand the need to keep passwords confidential and to avoid sharing them, keeping a paper record or recording them in a way that makes them accessible to unauthorised persons.

Systems development and maintenance

This is the responsibility of **MRS. MARIE BAXENDALE-DEPUTY/ ACTING HEADTEACHER.** Security issues are identified and considered at an early stage when procuring or developing new information systems. Input data is validated to ensure that it is correct and appropriate. Outputs and downloaded or uploaded data are checked for validity and integrity.

Business continuity management

This is the responsibility of **MRS. MARIE BAXENDALE- HEADTEACHER.** Business continuity management aims to reduce disruption to the running of the school that would otherwise be caused by, for example, natural disasters, accidents, equipment failures and deliberate actions. It applies to all business processes, not just those related to information management. Continuity plans, each with an identified owner, are in place within a business continuity planning framework that ensures that all the plans are consistent and a priority order exists.

Action	Responsibility: post-holder
Education and training of staff	**MRS. MARIE BAXENDALE-HEADTEACHER.**
Identification, documentation, agreement and implementation of emergency procedures for recovery and restoration	**MRS. MARIE BAXENDALE-HEADTEACHER.**
Conditions for activating the plans	**MRS. MARIE BAXENDALE - HEADTEACHER.**
Emergency, fallback and resumption procedures	**MRS. MARIE BAXENDALE-HEADTEACHER.**
Maintenance schedule for testing and updating plans	**MRS. MARIE BAXENDALE-HEADTEACHER.**

Compliance

Intellectual property rights (IPR)

Appropriate procedures are in place to ensure compliance with legal restrictions in the use of material in respect of which there may be IPR, such as copyright, design rights or trademarks. Software is usually supplied under a license agreement that limits the number of copies that can be made of the software. Controls are in place including: maintaining an appropriate inventory or asset register of software, maintaining proof of license ownership (e.g. licences, master disks, manuals, etc), controlling the number of users, carrying out checks that only authorised software is in use and applying sanctions against unauthorised copying of software.

Annex B1

Pupil use of systems

This is the responsibility of **MRS. MARIE BAXENDALE- HEADTEACHER.**

The school subscribes to the NAACE acceptable use policy as recommended by Lancashire County Council's Education and Cultural Services Advisory Team. Parental consent is obtained for use of the Internet (sample letter appended). Pupils sign up to an acceptable use policy (sample appended).

Use by the wider community

This is the responsibility of **MRS. MARIE BAXENDALE-HEADTEACHER.**

All users of ICT systems are required to sign up to the school's acceptable use policy and agree to abide by the protocols laid down for staff/pupils as outlined above.

Sanctions

This is the responsibility of **MRS. MARIE BAXENDALE-HEADTEACHER.**
All users – staff, pupils, other members of the wider school community are subject to sanctions *as outlined below* if misuse of the systems is encountered-

Follow the procedures outlined in the relevant policy-

- **The Disciplinary and Dismissal Procedure Policy for Teachers.**
- **The Disciplinary and Dismissal Procedure Policy for Support Staff.**
- **Behaviour Policy (for children).**

Lancashire County Council - ICT Security Policy for Schools

Procedural Aspects of the Policy

	Notes	Paragraph Reference
1.	The Governing Body must ensure that the school implements an ICT Security Policy - this can either be the 'model' policy or the school can create an amended policy based upon the 'model'. This must be reviewed annually and must include Email and Internet Use Policies for Staff and Pupils	Foreword
2.	The Headteacher must nominate a System Manager or members of staff with designated systems management responsibilities. This must be documented (*in Annex B1 of the model policy*) and included in the Scheme of Delegation approved by the Governing Body. It would not be unusual for the Headteacher to nominate themselves to act in this capacity, especially in small schools. The Headteacher must ensure that the nominated member(s) of staff understands the functions of the role and is familiar with the relevant Acts	4.4.1
3.	The Headteacher must compile a census of data giving details and usage of all personal data held on computer and manually (as required under the Data Protection Act 1998) in the school, and file a registration with the Data Protection Registrar. Users should be periodically reminded of the requirements of the Data Protection Act, particularly the limitations on the storage and disclosure of information.	5.2.1 & 5.2.2
4.	The Headteacher should ensure that a copy of the relevant 'Rules for ICT Users' (*attached as Annex C1-C3*) is issued to all system users. This should include all relevant aspects of the ICT Security Policy and any other information on the use of facilities and techniques to protect the systems or data.	6.4
	This will include Inappropriate use of Email and the Internet Breaches of security - reporting procedures Use of private hardware and software User authorisation process Access rights Equipment siting, room layout, physical security Appropriate use of the school facilities	 10.1 9.1 8.2 8.4 8.4 7.1 & 7.2 8.1

5.	The Headteacher should retain a record of the distribution of the 'Rules for ICT Users' - to Staff, Students and third parties; the access rights to systems and data granted to individual users; any amendments or withdrawal of these rights due to a change in responsibilities or termination of employment or starters/leavers; the training provided to each individual user.	6.5 6.2
6.	An inventory of all ICT equipment must be maintained and regularly updated by the Headteacher as equipment is purchased / disposed of. The inventory must be checked and verified annually in accordance with the requirements of Financial Regulations. (*Recommended Pro-forma attached as Annex B4*)	7.3.1
7.	The Headteacher should define local rules regarding the use of privately acquired hardware and software, which should be disseminated to all Users. This will also include use of non-approved email accounts.	8.2.1
8.	An inventory of all software and licence details must be maintained and regularly updated by the Systems Manager as software is purchased / disposed of. The inventory must be checked annually to ensure that the licences accord with installations. *(Recommended Pro-forma attached as Annex B5)* The Systems Manager should ensure there are clear procedures regarding the installing / copying of software. The System Manager should be familiar with the requirements of FAST (the Federation Against Software Theft)	5.4.4
9.	The Systems Manager should ensure there are clear procedures regarding installing, upgrading, repairing and disposal of equipment.	8.10 & 8.11
10.	The Systems Manager must decide on the appropriate frequency for password changes and advise on the technique for password selection based on the value and sensitivity of the data involved, and advise users accordingly. The Systems Manager must ensure there are clear procedures regarding the disposal of equipment and waste containing confidential or sensitive data.	8.6.1
11.	The Systems Manager must ensure that a Backup strategy is agreed, documented and implemented. Clear instructions must be given to Users to ensure this is followed. *(Recommended strategy attached as Annex B3)*	8.7.1
12.	The Systems Manager should confirm and implement a policy on anti-virus software for local networks, standalone systems, laptops and home PC's (particularly where data may be transferred to school). This must ensure that anti-virus software is regularly updated.	8.8.2
13.	The System Manager must distribute the "E-mail & Internet Use Policy for Schools" (*Annex A*) to all Users and ensure that they complete the relevant User declaration attached to the policy.	10.1

Annex B3

Lancashire County Council - ICT Security Policy for Schools

Backup Strategy

Administration:

All data is backed up nightly (Monday-Friday) to tape drive. Monday-Thursday tapes are then re-used during the following week. Friday's tapes are kept for 4 weeks before reusing. All tapes are replaced after one term. Ach night the previous days backup is stored off site and all other backups are stored in a fireproof safe.

Curriculum:

A full server backup is made to tape on a 4 weekly rota; the tapes are re-used after 3 backups, so there are 3 copies available at any one time. Fortnightly backups are also made to tape of the user data, these tapes are re-used after 3 copies are available. There is a long term backup up of the key software on CD and on hard drive.

Annex B4

Lancashire County Council - ICT Security Policy for Schools

Hardware Inventory

Curriculum Systems

Curriculum Overview

Total Number of File Servers (Excluding Dedicated Multimedia Servers)	1
Total Number of Other Servers	1
Total Number of Networked Workstations	12
Total Number of Standalone Workstations	
Total Number of Laptop PC's	32

Curriculum File Servers

	Server1	Server2	Server3
Manufacturer (Eg RM, CSE)	Fujitsu Siemens		
Model (Eg FX, RX)	Primergy Econel 50		
Network Operating System (Eg Windows NT, Novel)	Windows Server 2003		
Educational Management System (Eg RM Connect, CSE Resource Manager)			
Version (Eg 2.31)			

If any servers have been modified, please detail below:

Annex B4

Other Curriculum Servers (e.g. Dedicated Multimedia Server, Mail Server, Espresso Server etc)

	Type of Server	Type of Server	Type of Server
Manufacturer (Eg RM, CSE)	Network Edge Device		
Model (Eg FX, RX)			
Network Operating System (Eg Windows NT, Novel)	Linux		
Application / System	Espresso		
Version (Eg 2.31)			

Curriculum Workstations

Quantity	Manufacturer (Eg RM, CSE)	Model (Eg PC100)	Processor (Eg PII, AMD)	RAM	Operating System	Network/ Standalone/Laptop	Multimedia Capable	Internet Capable
10	Dell	Optiplex gx620	P4 3 Ghz	1 Gb	Windows XP Pro	N	Y	Y
2	HP	Compaq 6000	E7500 2.93 Ghz	2 Gb	Vista Business	N	Y	Y
12	Dell	Latitude D531	AMD 3600 2 Ghz	1 Gb	Windows Xp Pro	L	Y	Y
18	Dell	Latitude D505	Celeron 1.39 Ghz	1 Gb	Windows Xp Pro	L	Y	Y
2	HP	Compaq Nx7400	&5600 1.83 Ghz	1 Gb	Windows Xp Pro	L	Y	Y

Annex B4

Administration Systems

Administration Overview

Total Number of File Servers (Excluding Dedicated Multimedia Servers)	1
Total Number of Other Servers	
Total Number of Networked Workstations	2
Total Number of Standalone Workstations	
Total Number of Laptop PC's	

Administration File Servers

	Server1	Server2	Server3
Manufacturer (Eg Evesham,)	Stone		
Model (Eg Clone 5)	E7500 2.93 Ghz 4Gb		
Network Operating System (Eg Windows NT, Novel)	Vista Business		
Version (Eg 2.31)	Sp2		

If any servers have been modified, please detail below:

Other Administration Servers (e.g. Bromcom)

	Type of Server	Type of Server	Type of Server
Manufacturer (Eg Evesham)			
Model (Eg)			
Network Operating System (Eg Windows NT, Novel)			
Application / System			
Version (Eg 2.31)			

Administration Workstations

Quantity	Manufacturer (Eg Evesham)	Model (Eg PC100)	Processor (Eg PII, AMD)	RAM	Operating System	Network/ Standalone/Laptop	Multimedia Capable	Internet Capable
1	Dell	Optiplex GX 270	P4 2.8 Ghz	1 Gb	Windows Xp Pro	N	Y	Y
1	Dell	Optiplex GX 745	6300 1.86 Ghz	1 Gb	Windows Xp Pro	N	Y	Y

Annex B5

Lancashire County Council - ICT Security Policy for Schools

Software Inventory

Software Name/Title	Version	Publisher	No of Licences	Type of Licences	Licence No (if applicable)	Admin or Curric?	Age/KS Range
2CreateAStory		2Simple	25			C	KS1
2Email		2Simple	Site			C	KS1+
Audacity		Audacity	Freeware			C	KS2
Dance Ejay	2005	Ejay	25			C	KS2
Dazzle			25			C	KS1
Flowol	3	Keep I.T. Easy	25			C	KS2
Google Earth	4	Google	Freeware			C	ALL
Photostory	3	Microsoft	Freeware			C	KS2
Smartboard	10	Smart	6			C	ALL
Softease	6	Texease	25			C	ALL
Spex +	2	Aspex	Site			C	KS2
Office 2003		Microsoft	Site			A and C	KS2
Moodle		Moodle	Freeware			C	ALL
Anycomms			3			A	
SIMS.Net			3			A	
SIMS Finance			3			A	
Private Fund Manager			3			A	
School Fund Manager			3			A	
Teachers2Parents			3			A	

Note: Examples of Type of Licences are: Site licence, single user licence, concurrent user licence, multi user licence

Annex B6

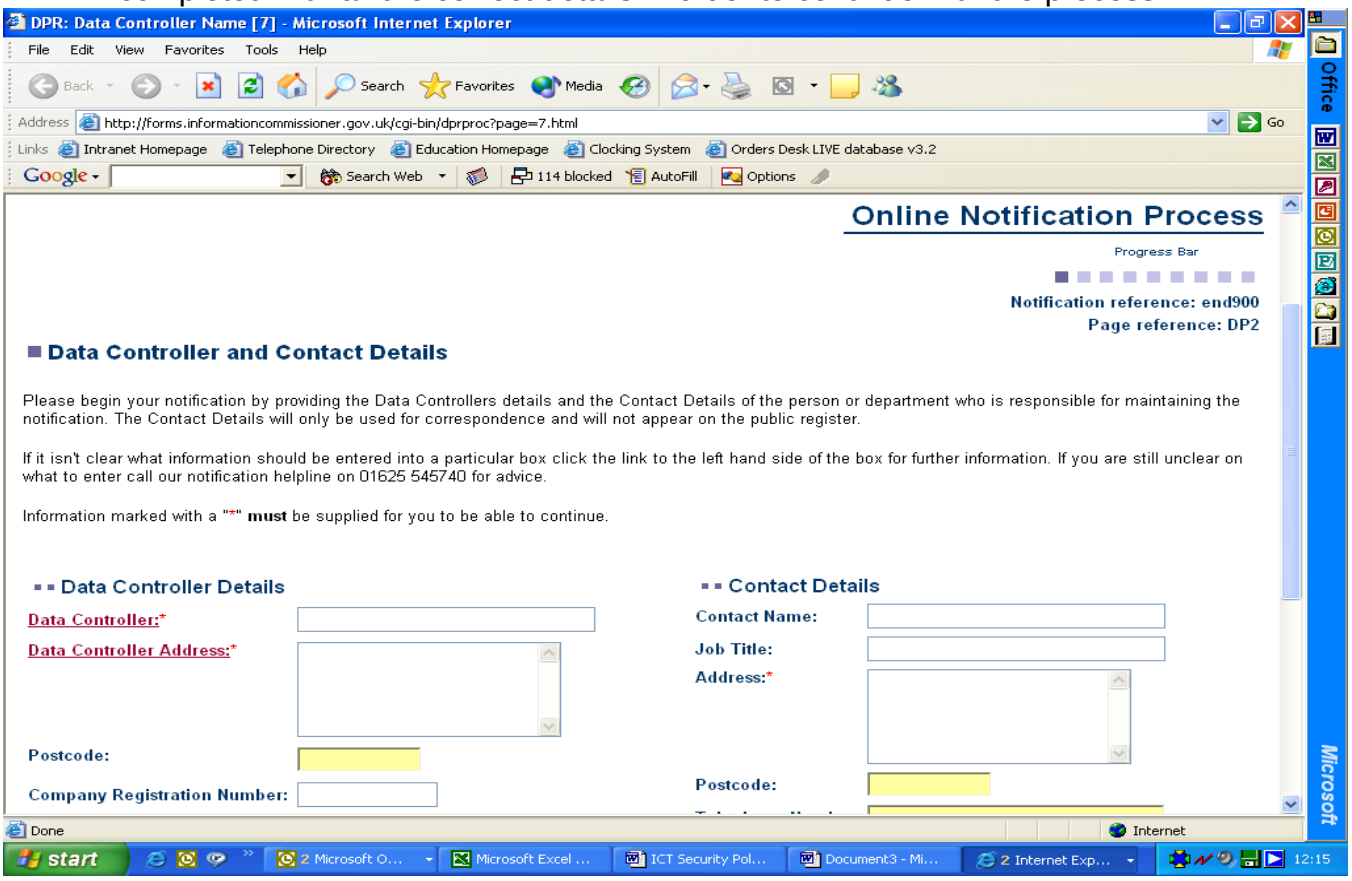
THE SCHOOL IS REGISTERED.

Guide on how to register details of your data processing with the Information Commissioner.

Click on http://www.informationcommissioner.gov.uk/eventual.aspx
Then Click on **Register / Notify** under the Quick Links Menu as shown below:

Read the guidelines and continue by clicking on **continue to Register / Notify** as below:

This should then take you to the online Notification Form. This needs to be completed with all the correct details in order to continue with the process



Once completed the form needs to sent to the Information Commissioners Office along with a fee of £35.

Annex B7

Lancashire County Council - ICT Security Policy for Schools

Security Guidelines

1. Password Policy

Passwords should be:

- unique
- alphanumeric
- at least 6 digits in length
- regularly changed, recommend at least every 90 days

Passwords should NOT be:

- written down
- easy to guess, don't use family or pet names for example

2. Monitoring Computer Use by Pupils

- Ensure Pupil use of computers is 'visual', make sure there is a Teacher present and monitoring use
- Consider logging access to the network using software tools, for example RM Tutor
- Review the layout of the room to ensure there is good 'visibility' of computer activities
- Ensure there is supervision at all times
- Publish the ‘Rules of ICT Use’ next to the computers, or consider displaying them on the screen when the computer is turned on
- Maintain an audit trail of User activity

3. Monitoring Computer Use by Staff (especially in sensitive areas)

- Use screensavers with passwords
- Consider using 'distinctive' background colours
- Think carefully about the siting / location of equipment
- Take care when disposing of paper output, floppy disks, computers etc that may contain sensitive or personal information

4. System Backup

- Make sure the system is backed up regularly and checks are made that the backup has worked
- Try to implement an automated system backup
- Make sure the instructions for re-installing data or files from a backup are fully documented and readily available
- Use 'off-site' storage for backup where possible
- Consider using different media as a secondary backup facility

5. Anti Virus Protection

- Always use an approved and recommended product **SOPHOS ANTI-VIRUS SYSTEM, is up to date & is updated by Lancashire.**
- Make sure there is a process to ensure it is regularly updated and ALL equipment is included, this is especially important for stand-alone PC's, laptops and PC's used at home
- Make sure there is a clear procedure for dealing with any actual or suspected infections
- Make sure the process for 'cleaning' infections is documented - this may involve requesting assistance from the County Council

6. Illegal or Inappropriate Use of the Network

- Make sure there are appropriate procedures in place for auditing access to the network and systems
- Regularly check the network for 'unauthorised' files
- If possible ensure auditing is performed both at the Management System level and also at the Operating System level (see section 11 below)
- Consider using appropriate software to assist with auditing - this can help monitor activities such as logons, file usage etc
- Consider using a firewall or proxy server to restrict external activity and access

7. Internet Use / Filtering

- Make sure an Internet Use policy has been adopted for each 'category' of User and all Users have signed up to it
- Define and document any local agreements / policies on restricting web sites, access to newsgroups and chat-rooms etc
- Obtain parental permission where appropriate
- Ensure there is a clear process for reporting any access to inappropriate material

- Consider restricting specific functions such as the downloading of .exe files
- Publish safe guidelines
- Make sure Internet use is supervised

8. Email Use

- Make sure an Email Use policy has been adopted for each 'category' of User and all Users have signed up to it
- Define and document any local policy on the use of email and email addresses, including the use of 'non-approved' email accounts
- Consider implementing limits on inbox sizes, size and types of attachments etc
- Be clear about what is considered 'appropriate' use of email and language
- Involve staff, parents and students in these decisions

9. Documentation

Ensure adequate documentation is available for

- The network infrastructure
- The network systems, hardware, software etc
- Administration procedures
- Housekeeping procedures
- Problem resolution

Ensure support disks, recovery disks, backups etc are available

10. Training

- Ensure there is adequate training for System Managers and Users
- Introduce 'good practice' guidelines where appropriate e.g. using screen savers with passwords
- Consider restricting the hours of use or physical access to systems
- **SEE CPD FILE IN HEADTEACHERS OFFICE.**

11. Authentication / Operating System Level Security

- Consider using system policies to provide additional security
- Ensure there is a rigorous policy for approval / removal of Users
- Avoid the use of 'generic' accounts
- Limit the number of Administrator and Manager accounts
- Avoid the use of Groups with Administrator or Manager rights
- Only log on as Administrator or Manager when performing functions requiring this level of access, use an ordinary level User account where this is not required
- Set clear security levels on the network and ensure these are documented and followed

- Restrict access to applications and data areas where appropriate
- Consider using 'read only' access where possible

12. Network Review

- Monitor system downtime, ensure there are support arrangements in place to react to problems with critical equipment or infrastructure
- Monitor performance of the network - ensure there is a process in place to develop and upgrade the network infrastructure and equipment as necessary
- Monitor service disruption - ensure support arrangements are in place to resolve problems in a timely fashion
- Regularly review appropriate documents e.g. Computer Security policy, Email and Internet Use policies, this could include reviewing official documents such as the BECTa 'Superhighway Safety'
- Review procedures for dealing with all security breaches or compromises, whether deliberate or innocent

Annex B8

Lancashire County Council – ICT Security Policy for Schools
Checking Specification of PC's

1. Memory - How much memory does the PC have?

How do you find out? Go to the Desktop
Right click on **My Computer** icon
Left click on **Properties**

This brings up a window with several tabs on it; it should default to the General tab and this shows the amount of RAM (towards the bottom of the window.) It may give the amount in Kb. To convert to Mb, divide by 1024.

2. Processor - What processor does the PC have?

How do you find out? Look on the outside of the processor box – there will be a label

with information about the PC e.g. PC-5166. The PC-5 indicates a Pentium 2 processor (PC-6 is a Pentium 3 etc) and the 166 indicates the processor speed is 166 MHz. Write down the information from the label.

3. Hard Disk - What size hard disk does the PC have?

How do you find out? Go to the Desktop
Double left click on **My Computer** icon
Right click on **C drive** or **[C:]**
Left click on Properties
This brings up a window with tabs on it; it should default to the **General** tab and this shows the capacity of the hard disk.

4. Operating System - What operating system does the PC have?

How do you find out? Go to the Desktop
Right click on **My Computer** icon
Left click on **Properties**
This brings up a window with several tabs on it; it should default to the **General** tab and this shows the operating system.

5. Microsoft Licensing - What version of Microsoft Office / Word is installed on the PC?

How do you find out? Left click on the **Start** button
Left click on **Settings**
Left click on **Control Panel**
Double left click on **Add/Remove Programs**

This brings up a window with a panel in it which lists all the programs on your computer. Use the scroll bar to go down the list to the Microsoft programs and you will be able to see whether Microsoft Word is installed and, if so, which version you have.

Annex C1

Lancashire County Council - ICT Security Policy for Schools

Rules and Agreements for Staff

Rules for ICT Users - Staff

	Notes	Paragraph Reference
1.	Ensure you know who is in charge of the ICT system you use, i.e. the System Manager.	4.5.1
2.	You must be aware that any infringement of the current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 Provisions of this legislation may result in disciplinary, civil and/or criminal action.	5.1.2
3.	ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of data held.	5.2.2, 6.2, 6.3 & 6.4
4.	Follow the local rules determined by the Headteacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be copied if specifically approved by the System Manager.	5.4.4 & 8.2.1
5.	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat. Do not leave you computer logged on, i.e. where data can be directly accessed without password control, when not in attendance. These same rules apply to official equipment used at home.	7.2.1
6.	You must not exceed any access rights to systems or limitations on the use of data granted to you by the System Manager.	8.4.1

7.	The System Manager will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use. You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a "made up" word, but not obvious or guessable, e.g. surname; date of birth. Do not divulge your password to any person, or use another person's password, unless specifically authorised to do so by the System Manager, e.g. in cases of shared access. Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle/drawer to which only you have access.	8.6.1
8.	The System Manager will advise you on what "back ups" you need to make of the data and programs you use and the regularity and security of those backups.	8.7.1
9.	Ensure that newly received floppy disks, CD ROMs and emails have been checked for computer viruses. Any suspected or actual computer virus infection must be reported immediately to the System Manager.	8.8.1 & 8.8.2
10.	Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, floppy disks, etc.	8.9.1
11.	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Headteacher, Chair of Governors or Internal Audit.	9.1
12.	Users of these facilities must complete the declaration attached to the "E-mail & Internet Acceptable Use Policy".	10.1

Annex C2

ICT and Internet Safety Consent Form

For Pupils

Key Stage 1

Think then Click

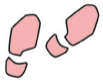
These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.



Together, we can send polite and friendly emails to other classes in school time.

Together, we can open polite and friendly emails from other classes in school time.

I promise that I will keep to these rules when I use the computer:

Signed:

Class:

Date:

Annex C2

Key Stage 2

Think then Click-

E-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites appropriate to our school work and homework.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we unsure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We know that the school may check our computer files and monitor the websites we visit.
- We will not access other people's files.

I promise that I will keep to these rules when I use the computer:

Signed:

Class:

Date:

Annex C2

ST JOSEPH'S CATHOLIC PRIMARY SCHOOL

RESPONSIBLE INTERNET USE

Dear Parents/Carers,

All pupils use computer facilities including Internet access as an e . learning, as required by the National Curriculum. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world.

We are currently reviewing our e-safety policy and are asking parents to read our attached **E-Safety Rules for Pupils – 'Think Then Click'**, and to **sign and return the consent form so that your child may have continued use of the Internet at school.**

We wish to reassure parents, that although there are concerns about pupils having access to undesirable materials, we take positive steps to deal with this risk in school.

Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and to assist parents we have added links to the parents' section of our school website which provide information on safe Internet access.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

We have arranged an 'Anti-Bullying and E-Safety' information evening for parents to be held on Wednesday 17th November at 7:00 p.m. Mrs. Christine Hulland and Mr. Christopher Bolton, two local authority consultants, will be joining us to share their expertise. A minimum of 10 parents will be needed to make the evening viable and therefore we are hoping for a positive response to this very important agenda. Please return the slip below if you would like to attend.

Should you wish to discuss any aspect of Internet use please contact either myself or Mrs.Baxendale (Subject Leader for ICT).

Yours sincerely,

Mrs. M.Baxendale
Headteacher

Anti-Bullying and E-Safety Evening

I/we would like to attend the Anti-Bullying and E-Safety Evening on 17th November at 7:00 p.m.

Names attending:……

Child/Children's name(s)

……

Annex A

St. Joseph's Catholic Primary School.

Our Rules for Email and Internet use.

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

Together, we can send polite and friendly emails to other classes in school time.

Together, we can open polite and friendly emails from other classes in school time.

Annex A

St. Joseph's Catholic Primary School.

Our Rules for Email and Internet use.

Key Stage 2

Think then Click-

E-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites appropriate to our school work and homework.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are unsure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We know that the school may check our computer files and monitor the websites we visit.
- We will not access other people's files.

Annex C1

St. Joseph's Catholic Primary, Wrightington.
Acceptable Internet Use Statement

For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school is keen to see staff make full use of the system, in order that they might broaden their skills and enhance their professional development.

The school's Internet Access Policy has been drawn up to protect all parties. Staff are reminded that inappropriate use of the internet could result in action being taken under the terms of the School's disciplinary procedure. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff and students requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the headteacher for approval.

Therefore, it is important that all staff familiarize themselves with the principles set out below-

- All Internet activity should be appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply.
- Under the terms of the Authority's Trade Union Facilities Agreement, reasonable use of computer facilities for authorised trade union representatives is permitted.
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems and laptops, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As e-mail 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.
- Your laptop must only be used for school related professional activity. It is not for personal use and must not be used by anyone else including family members or students.
- Files containing personal data relating to staff or students should not be held on the hard disk of your laptop, pen drives or other portable computer. Home access to the curriculum server is available using MyLGFL.
- Mobile phones must not be used to take photographs of children or of other members of staff.

- Photographs of children or other members of staff should not be placed on any social networking sites.

Full name : **Post:**

Signed: **Date:**

Access granted: **Date:**

Annex C2

St. Joseph's Blog
E-safety rules:

Don'ts:

1. Never give away any personal information about your location or identity.
2. Don't post pictures of yourself without specific permission from your teacher or parents.
3. Never give out your log in details to anyone.
4. Don't use text language in your posts.

Do's:

1. Post about whatever you like.
2. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
3. Comment on people's posts too. Blogging is about commenting and posting!
4. If your post doesn't appear straight away, your teacher might be busy, do be patient.
5. Try to post about things that your audience would like to read.
6. If you see anything that shouldn't be on your screen, do tell your teachers or parents immediately.
7. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.
8. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
9. Always tag your posts with your first name and include key words specific to your post.

Child consent:

I will follow the E-safety rules set out above when using St. Joseph's blog'.

Signed:_____ Date:_____

Parent consent:

I will ensure that my child follows the E-safety rules set out above when using St. Joseph's blog.

Signed:_____ Date:_____

Annex C3

St. Joseph's Blog
E-safety rules:

Don'ts:

1. Never give away any personal information about your location or identity.
5. Don't post pictures of yourself without specific permission from your teacher or parents.
6. Never give out your log in details to anyone.
7. Don't use text language in your posts.

Do's:

10. Post about whatever you like.
11. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
12. Comment on people's posts too. Blogging is about commenting and posting!
13. If your post doesn't appear straight away, your teacher might be busy, do be patient.
14. Try to post about things that your audience would like to read.
15. If you see anything that shouldn't be on your screen, do tell your teachers or parents immediately.
16. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.
17. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
18. Always tag your posts with your first name and include key words specific to your post.

Annex C4

FILTERING REQUEST FORM

MAKE SURE THAT YOU HAVE CHECKED THE SITE BEFORE THIS REQUEST, TO ENSURE THAT IT IS SUITABLE.

Name of person requesting website unblocking

_____

Website name

_____

Full web address

_____

Reason

_____

Date form submitted

_____

Signature of person requesting site to be unblocked

_____

Authorisation signature_____