



Winton Primary School

Acceptable Use Policy

School Network, School website, Internet and Intranet Facilities

Contents

Introduction	2
The school network	2
The makeup of the school network	2
Legitimate users	2
Legitimate use	3
Network access control	4
General comments	4
Pupils	4
Staff	5
Virus protection	5
Internet Access	6
General	6
The World Wide Web	6
Finding useful and authoritative materials	7
Protection from inappropriate material	7
Downloading of materials	7
Supplying personal details	8
E-commerce	8
E-mail	8
Staff E-mail	8
Pupil e-mail	9
E-mail attachments	10
School website	10
School Intranet	10
Monitoring and reporting misuse	11
Appendix 1 - The main points that staff need to remember	12
Appendix 3 - Information for parents about the school's Acceptable Use Policy	14

Introduction

This document is an addendum to the school's general ICT Policy. It addresses issues related to the acceptable use of the ICT facilities provided for children, staff, parents and governors to use. Specifically it deals with the use of the school curriculum network, the Intranet that runs on this network, the publicly available school web-site and the facility for access to the Internet provided through the network. It has been produced in accordance with National Association of Advisers for Computers in Education (NAACE) guidelines.

Acceptable use of these facilities implies use which:

- Safeguards individuals from offensive messages, personal or impersonal, in any medium capable of being held on a computer system, e.g. malicious e-mails messages, pornographic images, etc.
- Safeguards the anonymity of individuals (particularly pupils) and their computer-based work, when that is appropriate.
- Safeguards the integrity of computer based information held within the school or on behalf of the school.
- Safeguards the good standing and legal integrity of the school in terms of computer based information that is held publicly.

The school network

The makeup of the school network

The school network consists of a collection of PC computers connected together via Local Area Network (LAN) cabling to a Windows 2000 file server. A gateway to the Internet via router hardware and broadband connection to the South West Grid for Learning further enhance this network. The system runs various levels of software designed to provide security. There are a number of other handheld and portable computers in the school which are not permanently connected to the network, but which are considered to be within the scope of this policy as regards acceptable use. The network of computers provided for the office staff and the senior management team falls outside the scope of this policy however as these are controlled by the local authority.

Legitimate users

Legitimate users of the school network are:

- Current pupils
- All teaching staff including the Senior Management Team and Learning Support Assistants

- IT Technicians
- Governors
- Parents, when specifically authorised and supervised by a member of staff.
- Visitors, when specifically authorised and supervised by a member of staff, e.g. Local Authority officers, software engineers from support companies.

It is not envisaged that the system will be available for use by, for example, former pupils or cleaning staff.

Legitimate use

The network is designed specifically for educational use. This includes:

- Access to educational and administrative software packages
- Access to reference sources and the sharing of information within the school and outside.
- The storage of information, teaching materials and work products related to educational topics
- The display of good work
- Communications between people inside and outside the school for educational ends.

It is intended that the network be used right across the curriculum, not just for the ICT curriculum area, and also for administrative support to staff.

It is also envisaged that the network may be used for personal use in an endeavour to develop the general ICT experience of both pupils and staff, *but with the following provisos:*

- Personal use of the network must not involve the storage of information that would necessitate the registration of that data under the Data Protection Act. An example of this would be lists of personal data containing more than very basic attributes, e.g. a sports club subscriptions list.
- Personal use of the network must not in any way interfere with normal school operations. For example teaching staff and pupils should not be making personal use of the network during lesson time. Also personal use must not significantly impair the performance of the network or cause excessive amounts of resources to be used, especially printer ink, paper and disc storage space.
- The network must not be used for commercial use in any way.

Network access control

General comments

The network is to be kept secure using a variety of software products, reviewed regularly, which control access. Individuals gain access through a network wide username and password system (referred to as "logons"). This system will identify the category of user and the system resources to be made available to that user. *It is not acceptable to attempt to gain access to another logon without the permission of that user. Pupils must never be allowed access to staff or system administrator logons.* Repeated unsuccessful attempts to gain access to a logon result in the automatic suspension of that logon and will require the intervention of a system administrator. Details of such events are logged automatically.

It is the school's policy that direct dial up connection to the network from outside the school is not allowed. Firewall software is to be used ensure that access to the network cannot be gained from outside the school when the network is connected to the Internet. This protection is also is provided via SWGFL and the firewall located at Bournemouth Town Hall.

Pupils

Pupils in Reception will use a single logon that is controlled by teaching staff. Each pupil from Year 1 onwards will have an individual logon which they will keep throughout the remainder of their time at the school. They will all share a common password known to them all. In Key Stage 2 pupils will be allocated simple individual passwords. Whilst it is not imperative that these passwords are kept secret, Key Stage 2 children should have the general significance of security passwords explained to them and be encouraged to remember their password and keep it secret as a part of learning basic life skills. The ICT Co-ordinator will keep a record of these passwords and will supply them to staff should a child forget.

Pupils will only have access to software assigned to their year group, an inherent part of the network security system. Staff can request the addition or removal of software from a year group's applications list using the "Yellow Book" ICT support request system.

Pupils will have access to an area of personal disc space (known as the W: drive) where they can store, edit and delete their work. This area is accessible only by that pupil and by staff users. They also have read-only access to a public area of disk space (known as the R: drive) from which materials can be copied.

A specific folder (R:/Shared Files) gives full public update access to anyone on the network. This is intended as an area in which collaborative work can take place or where work can be assembled for the teacher to view. Pupils that use this folder need to be aware that they must be careful not to damage or delete the work of others.

Staff

Each member of teaching staff is assigned an individual logon. This must be kept secret, especially from pupils and outside visitors. Staff have the facility to update their passwords when they wish, and should do this regularly.

Staff also have full access to an area of personal disc space (known as the W: drive). This is completely private from pupils but is accessible by system administrators. Staff further have full access to the R: drive and it is here that they can place materials for children to view and copy.

System Administrators

The system administrators are a small group of staff, selected by the head teacher, who have overall responsibility for the maintenance and integrity of the network. These will usually include the ICT Co-ordinator and the ICT Technician. They have a set of logons that afford full access to the system and all its data, including the ability to change access control. *The passwords for these logons must never be divulged to anyone other than the system administrators, the senior management team and engineers from companies retained to carry out maintenance of the system, without the express permission of the head teacher.* These passwords are to be changed frequently.

Virus protection

Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses.

It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. *Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT Co-ordinator or the ICT Technician.*

Viruses can attach themselves easily to floppy discs and this is one of the main ways in which they proliferate. The software used to prevent pupils from tampering with various computer settings will also, to some extent, prevent them from accessing floppy discs. However this is not totally secure. Furthermore there are instances in which pupils and staff will want to transfer data to and from the network on floppy discs, e.g. as a means of submitting homework. *To allow for this and still ensure system security it is the school's policy that all floppy discs must be virus scanned by a system administrator before being inserted into any computer on the network.* These must be re-scanned again each time they are used in computer outside the network. Please give reasonable notice to system administrators when scanning is needed.

See later sections of this policy regarding Internet use for more details about virus protection considerations.

Internet Access

General

The Internet is destined to play an increasingly significant role in the education of the children at Winton Primary and the professional practice of the staff. For this reason access to the Internet is made available from any network computer in the school. However it is recognised that the Internet contains material which is unsuitable within a school context or which is offensive. Furthermore the enhanced communications facilities afforded by the Internet raises issues of privacy and personal safety. For this reason it is necessary to put in place a range of restrictions on the use of the Internet and all users of the network must be made aware of these.

The network offers the following Internet facilities:

- The World Wide Web - i.e. pages of text, images and sound linked together and accessible from computers all over the World.
- E-mail.

The following Internet facilities however are explicitly **not** to be used in school and are masked out by software:

- IRC - Usually known as "Chatrooms". These allow Internet users to chat to one another in real time and offer a high degree of anonymity to participants. Whilst there is a place for such a facility in an educational context, the risks inherent in conversations between children and anonymous individuals is much too great for this facility to be offered in its current form. The availability of more secure and supervised chat facilities will be kept under review.
- Usenet - publicly available on-line "noticeboards" or "news groups" in which threaded discussions about subject specific themes takes place via e-mail style messages. There are a number of these news groups that are specifically designed for the use of UK teachers and are quite useful. However Usenet is largely uncontrolled and is the source of much of the inappropriate and obscene material on the Internet. For this reason it is not allowed in school although this will again be kept under review.

The World Wide Web

The World Wide Web (WWW) should prove to be an invaluable resource for teachers and children and its use is to be greatly encouraged in all curriculum areas. However two important usage issues arise:

Finding useful and authoritative materials

The amount of information to be found on the WWW is vast and there are no controls on what is there and how authentic it is. This means that whilst sometimes a rich source of information can be found remarkably quickly, on other occasions hours can be spent in fruitless searching. The ability to sift and search is an essential ICT skill for Key Stage 2 children and needs to be taught specifically. On the other hand, for many Internet linked activities, protracted periods of searching will not lend themselves to the main learning objectives of the lesson. *For this reason staff should generally have searched for suitable web-sites in advance of a lesson and have checked their suitability and accuracy in just the same way as they would do with a book.*

Protection from inappropriate material

The protection of our pupils from inappropriate materials on the WWW is achieved through the use of software and staff supervision. The following measures must be in place:

- Our connection to the WWW must be through an Internet Service Provider that provides a basic level of filtering of inappropriate material.
- The school network must have an ability to filter out specific web-sites that we identify locally as inappropriate.
- Staff need to be active in observing where children are browsing on the WWW in case they are moving towards inappropriate areas.
- Any discovery of an unsuitable web-site should be reported to the ICT Co-ordinator so that the site can be filtered out.
- When asking pupils to use search engines to find suitable web-sites, child oriented search engines such as "Yahooligans" or "Ask Jeeves for Kids" should be used as far as possible.

Downloading of materials

The WWW affords many opportunities to download items of data or software free of charge and this material can often be very useful. However caution must be exercised as such downloads can be the source of viruses and other malicious content. The following practices should be followed:

- Children must never download anything without permission from a member of staff.
- Staff can download, or allow to be downloaded, the following materials freely:
 - Text (*but not Microsoft Word files*), pictures, databases, etc. that do not contain any executable elements.
 - "Plug-ins" - These are computer programs which extend the ability of a web browser to display different types of graphics and sound. The usually download and install themselves automatically if the use approves. The network will

already support the most common plug-ins but new ones can be added as needed.

- The following materials must be virus-checked by a system administrator before they are used in any way. *Any form of use of these materials before they have been checked could lead to the destruction of large amounts of the school's data!*
 - Any executable program.
 - Microsoft Word files as these can contain executable elements hidden in the document.

Supplying personal details

Often web-sites can ask for personal details to be supplied. For example an educational web-site might ask for a user's e-mail address so that a regular newsletter can be sent to the user. Staff may supply personal details at their discretion. On the other hand *pupils must be taught that they must never supply any details about themselves or the school unless they have consulted a member of staff first.*

E-commerce

E-commerce is a growing area of the WWW and facilitates the buying and selling of goods on-line. No sales or purchases of any kind must be made via the school network without the permission of the Head Teacher.

E-mail

Staff E-mail

Every member of the teaching staff is allocated an e-mail address for their professional use. This address uses the schools British Educational Communications & Technology Agency (BECTa) registered domain name for the school, which is currently:

@wintonprimary.bournemouth.sch.uk

but may well be changed in the future to the registered name of:

@winton-pri.bournemouth.sch.uk

The school also has e-mail addresses assigned to it by Bournemouth Borough Council with a domain name of @bournemouth.gov.uk. These are used by the office staff and the Senior Management Team only and are likely to be phased out in the near future.

Staff E-mail is web-based rather than held on a mail server in the school so that staff can access their e-mail from home as well as at school.

Pupil e-mail

An e-mail account will be provided for every pupil in Key Stage 2, and a class e-mail account for each Year 2 class. The school has adopted the British Telecom Talk21e e-mail service for the following reasons:

- The school can specify a list of e-mail domain names that the pupils can send mail to and receive mail from. Pupil e-mail accounts will be completely inaccessible outside these domains. This list can include other BT Talk21e schools, all of which will have had their authenticity checked prior to service registration.
- The e-mail addresses are short i.e. childname@talk21.com and also anonymous. It will not be possible for someone to guess the pupil's e-mail address if they know their name and the school they go to.
- The service is web-based so that children can access their e-mail from home as well as at school.
- The service is free.

The ICT Co-ordinator will maintain the list of domain names that the children can send to and receive mail from. Requests for changes to this list can usually be dealt with at short notice. Despite these security measures staff must still be sure that they do not accidentally disclose children's e-mail addresses to anyone other than legitimate correspondents. For example, do not put up a list of e-mail addresses in a classroom.

It is very important that pupils are taught about the dangers of e-mail and reminded of these dangers at the start of each academic year. The issues that should be covered are:

- That the people they are communicating with should be known to them and also to school staff and/or parents.
- That they should never reply to a message from somebody they do not know and that when they receive such a message they should tell a teacher or their parents immediately.
- That they should report anything they consider to be abusive, upsetting or inappropriate in an e-mail message to a teacher or parent immediately and not respond to the message.
- That they should never give out personal details such as their address or telephone number in an e-mail.
- That their e-mail is not private and that staff and parents must have access to it.
- That they themselves must never include abusive, upsetting or inappropriate material in any message that they send.

E-mail attachments

It is possible to attach any number of computer files to an e-mail message. This is very useful and could be used, for example, for a child to submit a piece of homework done on a home computer to his or her teacher. However these attachments do provide another way viruses and other malicious computer code to enter the school's network. *For this reason e-mail users must never open or execute attachments from unknown correspondents.* These should instead be deleted straight away. If staff are at all unsure about other e-mail attachments then they should ask a systems administrator to examine the files and run a virus check if necessary.

School website

The school web-site will be published at BECTa registered domain name

www.wintonprimary.bournemouth.sch.uk

Editorial control of this web-site remains with the Senior Management Team with day to day management of the site being performed by the system administrators. This site will target a wide audience including the pupils, parents, staff and governors of the school, other schools and casual visitors from around the world. It aims to have the following content:

- Information for visitors
- Information for parents and prospective parents, including an on-line version of the prospectus and our OFSTED reports.
- Displays of good work from our children
- Curriculum materials and guidance to help our children with homework
- General items of school news including celebrations of success in competitions and fund raising events.

It is the school's policy not to identify the full names of children on this web-site, as a means of protecting privacy. First names only must be used to annotate pictures, good work, sports results, etc.

A single e-mail address, enquiry@wintonprimary.bournemouth.sch.uk, will appear on the web-site. This address will be monitored by office staff and messages forwarded to the appropriate staff. The site will also have a guest-book facility, which will be open to all.

School Intranet

The school's curriculum Intranet is available to all staff and pupils and can be openly accessed throughout the network. It aims to have the following content:

- Displays of good work.
- Reference materials for children in a well-indexed and searchable form.
- Teaching activities and resources related to particular year groups.
- School news for children including club and sports items.
- Games, puzzles and similar activities to promote computer use at break times.
- On-line discussion forums.

The Intranet will contain a secure "staff room" section, accessible via a staff logon, with the following extra content:

- Calendar
- All policy documents and related materials
- Schemes of Work and Units of Work
- Reference materials

The ICT Co-ordinator will manage the Intranet, but there should be an ethos of openness and joint ownership. Hence all pupils and staff are encouraged to produce content and software to make the production of this content easy should be made available. Because the Intranet is private to the school pupils full names can be used openly.

Monitoring and reporting misuse

It is the responsibility of all users of the school's network to report breaches of this Acceptable Use Policy. In addition the system administrators will routinely examine the log files kept by various pieces of network monitoring software to identify potential problems. Examination of staff files and e-mail however will only take place with the permission of the Head Teacher.

Breaches of the Policy should be reported to the ICT Co-ordinator in the first instance, who will report to the Senior Management Team if a breach is confirmed. The Senior Management Team will make decisions on appropriate sanctions.

Appendix 1 - The main points that staff need to remember

- Don't divulge your staff logon password under any circumstances and change it if you think it has been compromised.
- Don't leave a computer unattended and logged on to a staff logon.
- Make sure that personal use of the network does not interfere with normal school operations.
- Explicitly teach children the points laid out in Appendix 2 i) at the start of each academic year and ii) when relevant computer based activities are about to begin.
- Actively monitor the web-sites that children are visiting during open web-browsing sessions and do not leave a group unsupervised.
- Try wherever possible to visit web-sites before you use them in your teaching so that you can check their acceptability.
- When children are to use a search engine, try to make it one that has been developed for children.
- Report any inappropriate web-sites that you find to the ICT Co-ordinator so that they can be filtered out.
- Never divulge the "www" logon password and ask for it to be changed if you think it has been compromised.
- Actively monitor pupils' e-mail messages.
- Always respond to an on-screen virus warning. Isolate the machine and inform the ICT Co-ordinator immediately.
- Always get floppy disks scanned before using them on the network.
- If you download any executable programs or Microsoft Word documents, have them virus checked before you open them or execute them. The same applies when this type of file has been e-mailed to you by someone that you know.
- Never open or execute a file sent to you by someone that you don't know. Delete it immediately.
- Do not buy or sell anything via the school network without the permission of the Head Teacher.
- Be careful not to divulge pupil e-mail addresses accidentally.

Appendix 2 - What pupils need to be taught about acceptable use

Obviously these teaching points will need to be modified relevant to the age of the children and to the extent of their use of the network.

- Always log off when you have finished using a computer.
- Never disclose your password.
- Do not log on as anyone else without his or her permission.
- If you get a message on the screen about a virus, stop working and tell a teacher straight away.
- Don't put floppy discs into the school's computers. If you want to use one, discuss it with a teacher.
- If you see anything on the Internet that you think is upsetting or rude, show it to a teacher straightaway.
- Do not give your e-mail address to anybody, particularly a stranger, without asking your teacher first.
- Never type your name, address or other personal details in on a web page without asking permission first.
- If you receive an e-mail from somebody that you don't know, tell a teacher straight away.
- Never tell anyone private details about yourself in an e-mail, especially your address and telephone number.
- Remember that the school rules about being kind and considerate in what we say to others applies to e-mail as well.
- Be aware that their e-mail is not private and that teachers may look at what they have written.
- Be aware that the network can detect misuse of the computers and record details of the person responsible.
- Never download files or programs from the Internet without getting permission from a teacher.
- Tell a teacher about any files attached to an e-mail that they were not expecting to receive.
- Be careful not to change or delete other people's work in the R:\Shared Files folder.

Appendix 3 - Information for parents about the school's Acceptable Use Policy

To be agreed.

Author: Ian Finlay

Last Updated: 21st April 2002 by Jonathan Mitchell