

# Atwood Primary School

## Acceptable Use of the Internet Policy



This document is a statement of the aims and strategies for the use of the Internet at Atwood Primary School. It should be read in conjunction with the London Grid for Learning (LGfL) Acceptable Use Policy (Appendix 3).

### **The School's Internet Connection**

The Internet is provided by a Broadband (10Mb) connection to the London Grid for Learning.

### **How will email be managed?**

The government encourages the use of email as an essential means of communication. Directed email use can bring significant educational benefits and interesting projects between schools. However, the use of email requires that appropriate safety measures are put in place. Unregulated email can provide a means of access to pupils, which bypasses the traditional school boundaries. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content and viruses can be used to control and monitor material. At Atwood Primary School:

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in email communication.
- Pupils' email addresses do not give the full name of the child, and they contain numbers which are irrelevant to an outsider.
- In some cases a 'group' email address may be used.
- The email address of a pupil will not include any indication of the location of the school.
- Access in school to external personal email accounts are blocked (eg Hotmail accounts)
- The forwarding of chain letters is banned.
- Pupils are encouraged to use their school email account outside school to deter them from using typical 'Hotmail' accounts.
- All email (both incoming and outgoing) is checked for banned words and for viruses. Any breach of content is reported and dealt with.
- Pupils and staff should be aware that school email may be monitored.

## **How should Web site content be managed?**

The security of staff and pupils is essential. The publishing of pupils' names with their photographs is not acceptable where names of individual children can be deduced; web images could be misused and individual pupils identified. Strategies include using relatively small photographs of groups of pupils and using photographs that do not show faces at all. A check should be made that pupils in photographs are appropriately clothed. Photographs of a pupil should not be published without the parent/carer's written permission. At Atwood Primary School:

- The point of contact on the Web site should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

## **How will Internet access be authorised?**

The school will allocate Internet access for staff and pupils on the basis of educational need. Parental permission must be gained before access is permitted. This will be obtained through the home-school agreement when it is updated. At the moment it is obtained through a permission slip.

## **How will the risks be assessed?**

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. Associations and Societies dealing with issues of child Internet use may be consulted.

## **How will filtering be managed?**

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. At Atwood Primary School:

- The school will work in partnership with parents, the LEA, DfES and LGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to LGfL via the ICT co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## **How will the policy be introduced to pupils?**

Pupils should be reminded of the school rules at the point of Internet use. See appendix 2 for rules written for pupils. This should be printed as posters for rooms with Internet access.

- Rules for Internet access will be posted near all computer systems (see Appendix 2).
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Responsible Internet use will be included in the PSHE programme covering both school and home use.

## **How will staff be consulted?**

Internet use is widespread and all staff should be included in appropriate awareness raising and training. Internet use should be included in the induction of new staff.

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school (see Appendix 1).
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in the safe and responsible Internet use and on school Internet policy will be provided as required.

## **How will complaints regarding Internet use be handled?**

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.

## **Monitoring and review**

The procedures in this policy will be monitored in the light of any new information and guidance which becomes available. It was developed during the Autumn Term 2004 and was approved by the governing body in November 2004.

The policy will be reviewed annually and will be part of our school improvement plan.

**Last reviewed: September 2007**

## **Bibliography**

Kent NGfL website

Park Hill Junior School Internet Policy



Atwood Primary School

# Responsible Internet Use

## Rules for Staff

The school computer system provides Internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Users are responsible for email they send and for contacts made.
- Email should be written carefully and politely. As messages may be forwarded, email is best regarded as public property.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private purposes, unless the head teacher/ ICT co-ordinator has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of Emails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.



Atwood Primary School

# Responsible Internet Use

**We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.**

- **I will ask permission before entering any Web site, unless my teacher has already approved that site.**
- **I will use only my own login and password.**
- **I will only email people I know, or my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **When sending email, I will not give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an email or an email attachment sent by someone I do not know.**
- **I will not use Internet chat rooms.**
- **If I see anything I am unhappy with or I receive messages I do not like, I will tell my teacher immediately.**
- **I know that the school may check my computer files and may monitor the Internet sites I visit.**
- **I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.**

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of Email and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.



## **LGfL Acceptable Use Policy**

---

### **1. BACKGROUND AN DEFINITIONS**

1.1 This policy describes Acceptable Use of the London Grid for Learning.

### **2. INTERNET ACCESS AND USAGE POLICY**

1.0 All users are required to follow all the conditions laid down in this policy.

2.0 Use of the Internet and LGfL mandated services, such as the electronic mail service, are primarily intended for educational and government purposes only.

### **3. Acceptable Internet Use Guidelines**

1.0

2.0 Private use of the Internet should be agreed within the connecting organisation and will be subject to the same guidelines and policies as professional use of the services being provided by the LGfL

3.0 Electronic ordering on the internet must be in line with the financial requirements and procedures of the connecting organisation

4.0 Adults competent in using the Internet should supervise students Internet sessions and take steps to monitor, and where appropriate, record this usage.

5.0 Access by children should always be in 'public' areas where screens are visible

6.0 Internet use in educational establishments should be driven by clear learning intentions that are set in the context of well framed tasks.

7.0 Students should not be given access to Newsgroups or 'chat areas' unless using areas specifically designed for safe use and they are supervised. By default, the LGfL will minimise access to such facilities.

- 8.0 No personal details should be given out over the Internet except in carefully approved circumstances (e.g. joint projects). 'Web names' are a useful way of shielding real identities.
- 9.0 The connecting organisation will keep its anti virus software up to date to ensure that activities are not disrupted by malevolent actions by others.
- 3.1 Employees of connecting organisations receiving questionable materials should report these immediately to the appropriate member of their organisation and, where appropriate, [filtering@lgfl.net](mailto:filtering@lgfl.net).
- 11.0 All Internet users should be aware that all access is logged, and that any material accessed may subsequently be viewed by other users as well as the system administrator.
- 12.0 Connecting organisations should consider entering into a “contract” with pupils and parents to regulate local internet use via the London Grid for Learning
- 13.0 Connecting organisations should consider entering into a contract with staff to regulate the use of the Internet
- 14.0 The organisations personal computers (including portables) must only be used to access the LGfL using the mandated routing and inter site policies.
- 15.0 Any software downloaded from the Internet should be appropriately virus checked, licensed and registered.

#### 4. Unacceptable Usage Guidelines for the Internet

The following actions are considered unacceptable:

- 1.0 The access to or creation, transmission or publication of any offensive, obscene or indecent images, sounds, data or other material.
- 2.0 A breach of confidentiality that results in information being inappropriately displayed or made available to others;
- 3.0 The access to or creation, transmission or publication of any data capable of being displayed or converted to such obscene or indecent images, sounds, data or other material.
- 4.0 The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety.
- 5.0 The creation, transmission or publication of defamatory, violent, abusive or homophobic material.

- 6.0 The receipt or transmission of material such that this material infringes the copyright of another person or infringes the conditions of the Data Protection Act 1984 and revised in 1998.
- 7.0 The transmission of unsolicited commercial or advertising material to other users of the Internet or any other network reachable via the Internet.
- 8.0 The deliberate unauthorised access to facilities, services, data or resources within the connecting organisation any other network or service accessible via the Internet.
- 9.0 Deliberate activities with any of the following characteristics or that by their nature would result in:
- wasting staff or other users efforts or network resources, including time on remote systems and the efforts of staff involved in the support of those systems
  - corrupting or destroying other users data
  - violating the privacy of other users
  - disrupting the work of other users
  - using the Internet in a way that denies service to other users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large image files).
  - continuing to use any item of software after being requested to cease its use because it is disrupting the correct functioning of the school's network or the Internet (for example, utilities designed to broadcast network- wide messages)
  - the introduction of viruses
- 10.0 Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the London Grid for Learning's resources.
- 11.0 Any use of the Internet that would bring the name of the Connecting Organisation and / or the LGfL into disrepute
- 12.0 Purchasing or ordering items on the Internet without the appropriate authorisation or due regard to the financial policies and procedures of the connecting organisation

## **5. INFORMATION ON THE WORLD WIDE WEB**

- 1.0 Connecting organisations are reminded that publishing material on the world wide web makes it widely available and that as such due care and diligence must be taken to ensure that any communication via this medium is regulated.
- 2.0 Connecting organisations are advised when designing web sites to avoid publishing pictures of individual pupils with personal information about them. This will ensure that their privacy is protected and ensures that strangers will not be able to approach them outside school with information they have taken from the school web site. Where decisions are made to include images of individual children then this must be authorised by the legal guardian of the child.
- 3.0 One or more employees in the connecting organisation should take responsibility for vetting data before it is uploaded to a London Grid for Learning web site to ensure the data is in line with local policies and best reflects the character of the connecting organisation. As part of this process the connecting organisation will also be responsible for ensuring that the ownership, accuracy and copyright of the material is appropriate prior to publication.
- 4.0 Connecting organisations must take steps to ensure that inappropriate material is not published, that copyright is not infringed and that defamatory and homophobic information is not published. It is the responsibility of connecting organisations to ensure that management procedures and monitoring processes are in place to prevent the circumstances above from arising.
- 5.0 The web site should reflect the work of connecting organisation and web authors should attempt to seek contributions from all teachers, year groups, head teacher, governors, parents and the local community.
- 6.0 Most good web publishing software have spellcheckers. It is advisable to ensure that work is spell checked before uploading to a server.
- 7.0 Users are encouraged to write material in 'Plain English'
- 8.0 Copyright: When using images from other sites it is advisable to seek permission first. This can be done by sending an EMail to the contact name on the Web site.
- 9.0 Connecting organisations should note that any data originating from their organisation or relating to business conducted by, or on behalf of them, and which is transmitted by the internet remains the property of the connecting organisation. The copyright or other intellectual property rights attached to that data are unaltered in any way.

- 10.0 The London Grid for Learning cannot be held responsible for any transgression of national laws regarding the copyright and publication of material where officers have acted without Counsel or due regard to the provisions of this policy and other appropriate documentation.
- 11.0 The connecting organisation will respect the privacy and confidentiality of any data or other material published on the internet and must be mindful that same restraints apply to the Internet based communication as to any other medium.
- 12.0 LGfL recommend that each page of the web site should be consistent in terms of design, layout, graphics and fonts. This will make it easier for users to read and navigate the site.

## **6 GUIDELINES FOR ELECTRONIC MAIL USE**

A code of conduct:

- 6.1 Ensure that procedures are in place to ensure that your inbound and outbound mail is virus free, and ideally, can identify and block the transmission of unsuitable information.
- 6.2 Regularly housekeep your email deleting mail that is no longer required ;
- 6.3 Do not transmit personalised or financial data over the internet unless it is encrypted or appropriately scrambled.
- 6.4 Report unsolicited mail (“spamming”) to [filtering@lgfl.net](mailto:filtering@lgfl.net)
- 6.5 Do not delegate digital signatures or electronic pin numbers / identifiers to colleagues
- 6.6 Make arrangements for ensuring that email is forwarded to a trusted colleague in your absence to ensure that important messages and transactions are not lost. (However, NEVER redirect mail without advising them first!)
- 6.7 Do not print email unnecessarily, as this will minimise the environmental benefits of using electronic communication. (The exception is email that may be used in legal proceedings which should be printed off as mail administrators may have procedures which automatically remove mail that has been read after a set number of days)
- 6.8 Inappropriate use of the courtesy copy function should be discouraged. Mail should only be copied to those parties that have been involved in previous communication and need to be involved in the communication process.
- 6.9 Sharing common mail accounts should be discouraged

- 6.10 Ensure that confidential mail items are clearly identified as such (e.g. in the subject field)
- 6.11 Carefully check emails before sending
- 6.12 Avoid expressing strong feelings of disagreement in public forums (use an individual's private mail box)
- 6.13 Be careful about copyrights and licences
- 6.14 Ask permission before forwarding or copying other people's messages
- 6.15 Avoid sexist, racist, violent , abusive and homophobic language as you would in any other context
- 6.16 Avoid writing messages using ALL upper case letters
- 6.17 If the message is very important, controversial or open to misunderstanding, consider a face to face discussion or a telephone conversation instead
- 6.18 Select the right forum - private mail or conference
- 6.19 When joining a conference which has been in existence for some time, read through all the contributions to date to avoid asking a question or making a point which has already been made
- 6.20 Connecting organisations should consider putting a standard disclaimer on email

**To make sure your messages are read:**

- 21.0 Make sure the title of your message is relevant; if you are starting a new topic, change the subject line
- 22.0 Get to the point quickly, as this way more people will read your messages
- 23.0 Keep messages short
- 24.0 Use short paragraphs as they are easier to read on screen. Double line spaces between paragraphs help, and bulleted or numbered lists are a good way to display separate ideas.

**7 LONDON GRID FOR LEARNING ANTI VIRUS POLICY**

- 1.0 This policy document outlines responsibilities and methods for ensuring that schools do not jeopardise the integrity and security of the computer systems in the London Grid for Learning. All employees of connecting organisations should be aware of the guidelines and recognise that breaching them may result in disciplinary action.

- 2.0 All users and organisations connecting to the London Grid for Learning must ensure that their systems are protected by anti virus measures, that processes are in place to ensure the anti virus systems are kept up to date in line with supplier recommendations and that the organisation has the technical capability to maintain its anti virus system.
- 3.0 Malicious software can be categorised into four main types of code, namely Viruses, Logic Bombs, Trojan Horses and Worms.
- Virus type code attaches itself to a program (as opposed to data) file on a disc, or onto the “boot sector” which is read by the PC when it first starts up.
  - Logic Bombs are activated when certain criteria are met, e.g. the date being Friday 13<sup>th</sup>
  - Trojan Horses are contained within, as opposed to attached to, existing software (including viruses) and cause extra instructions to be executed, for example copying usernames and passwords to a hidden file which the perpetrator can access later in order to breach security,
  - Worm code is similar to Virus code but is able to exist on its own (i.e. without being attached to another file). Worms replicate themselves, then destroy the “mother copy”, which gives the impression that the software is moving about the disc, until the disc eventually fills up.

## **1.0 Sources of Virus Infection**

- 1.0.0 Research has shown that Viruses tend to be written by Students, Computer Hobbyists or Disgruntled Employees. The latter group directing their attacks specifically at their employer's (or former employer's) organisation.
- 2.0.0 The vast majority of viruses are unwittingly introduced to an organisation from an external source. Common routes are:
- discs brought in from home
  - free software from PC magazines
  - demonstration and evaluation software
  - files and software downloaded from the Internet
  - engineer's discs

3.0.0 Once introduced, viruses are easily transferred from one PC to another by means of a floppy disc or as email attachments.

### **7.3 GUIDELINES FOR PREVENTING CORRUPTION OR LOSS OF DATA THROUGH COMPUTER VIRUSES**

1.0.0 All systems connecting to the London Grid for Learning must have anti virus software installed and have procedures in place to keep the software up to date

2.0.0 All new computers purchased must be certified Virus-Free on delivery

3.0.0 All ICT contractors on a connecting organisations site will be expected to work within the London Grid for Learning guidelines and should use virus free software and disks

4.0.0 The connecting organisation must have procedures in place for ensuring that anti virus software is updated on a regular basis

5.0.0 All existing PC's must have recommended Anti-Virus software loaded and scanning enabled for both the hard drive and the floppy disk

6.0.0 Until such time as all PC's within a given area have Anti-Virus enabled, it is the responsibility of the connecting organisation to have a stand-alone PC available for the validation of all incoming discs and CD-ROMS.

7.0.0 PCs used from home to connect directly to the London Grid for Learning or resources within the London Grid for Learning must have Anti-Virus software loaded and scanning enabled.

8.0.0 All incoming discs must be scanned prior to loading either automatically or through the stand alone system designated for this purpose.

9.0.0 Software must only be purchased from the approved suppliers, or in accordance with connecting organisation procedures and must be certified virus-free.

10.0.0 Blank discs must only be purchased from suppliers who certify that they are virus-free.

11.0.0 Unsolicited or unauthorised software must not be loaded on the connecting organisations computers.

#### **Elimination of Virus Infection**

1.0.0 On detection of a virus infection, staff must immediately take steps to contain the virus and prevent its spread outside the connecting organisation.

- 2.0.0** Any virus infections on system should be recorded. The record should contain the date of the infection, the virus encountered, the PCs affected and where possible identify the source of the virus.
- 3.0.0 Infected system must be immediately disconnected from the London Grid for Learning
- 4.0.0 Disinfection of virus infected systems must only be carried out by suitably qualified staff within the schools.