

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 available throughout the school as the whole school is networked (cabled). Wireless connectivity is being increased over time and as funding becomes available.

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 (eg smitj068.306@lgflmail.net - this would be John Smith).
- 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 (e.g. 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' or other free 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.
- Permission to publish photographs of pupils on the school Web site will be obtained from parents through the home-school agreement.

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.

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 LA, DfE 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 via the ICT co-ordinator, and will be blocked.
- 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?

At the beginning of each academic year teachers will discuss in detail internet safety with their class and children will sign an agreement which is to be displayed in the classroom by the point of internet access. See appendix 2 for rules written for pupils. This should be printed as posters for rooms with Internet access. The children will also be given time to explore CEOPs 'Think U Know' site to learn more about e-safety.

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.

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

Atwood Primary School



Acceptable Use of the Internet Policy

Appendix 1
Responsible Internet Use

Rules for Staff

- I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head Teacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address or social network details (such as Facebook) to current or ex pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

Atwood Primary School



Acceptable Use of the Internet Policy

Appendix 2
Responsible Internet Use

Rules for pupils

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.

Atwood Primary School

Acceptable Use of the Internet Policy

Appendix 3

	Name of School	Atwood Primary School
	Policy review Date	October 2010
	Date of next Review	October 2013
	Who reviewed this policy?	ICT Manager/Governing Body

London Grid for Learning (LGfL) Acceptable Use Policy and related Technologies

ICT in the SEF

3a - the extent to which information and communication technology (ICT) capability and other key skills enable learners to improve the quality of their work and make progress

4b - the extent to which learners adopt safe and responsible practices in using new technologies, including the Internet.

4e - through the development of literacy, numeracy, information and communication technology, enterprise capability, economic and business understanding and financial capability

We have a duty to ensure that all students are able to make a valuable contribution to society & this is impossible to achieve if we do not ensure that students develop and apply their ICT capability effectively in their everyday lives.

SRF elements – working towards ICT Mark

1c-4 Safeguarding

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

3b-2 Effective and safe use of digital resources

Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices

*Harnessing Technology: Transforming learning and children's services*¹ sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Green Paper *Every Child Matters*² and the provisions of the *Children Act 2004*³, *Working Together to Safeguard Children*⁴ sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

¹ <http://www.dfes.gov.uk/publications/e-strategy/>

² See The Children Act 2004 [<http://www.opsi.gov.uk/acts/acts2004/20040031.htm>]

³ See Every Child Matters website [<http://www.everychildmatters.gov.uk>]

⁴ Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / <http://www.hi5.com> / <http://www.facebook.com>)
- Video broadcasting sites (Popular: <http://www.youtube.com/>)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, <http://www.miniclip.com/games/en/>, <http://www.runescape.com/> / <http://www.clubpenguin.com>)
- Music download sites (Popular <http://www.apple.com/itunes/> <http://www.napster.co.uk/> <http://www.kazaa.com/>, <http://www.livewire.com/>)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

*Ref: Becta - E-safety Developing whole-school policies to support effective practice*⁵

⁵ <http://schools.becta.org.uk/index.php?section=is>

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **e-Safety Co-ordinator** is Christine Lamont

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)⁶. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance⁷ on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- e Bullying / Cyber bullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-Safety matters at least once a year.

⁶ <http://www.ceop.gov.uk/>

⁷ Safety and ICT - available from Becta, the Government agency at:

http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

Schools should include e safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

Schools should ensure that they make efforts to engage with parents over e-safety matters and that parents/guardians/carers have signed and returned an e-safety/AUP form.

4. Communications

How will parents' support be enlisted?

A partnership approach with parents will be encouraged, including parent evenings with demonstrations and suggestions for safe home Internet use.

5. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- interview with e-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.