

Poulner Junior School

E learning Policy

Version	Date	Description
1.0	July 2010	

Review September 15

Introduction

The E-LEARNING Policy has been prepared by the School Leadership Team in consultation with the ICT co-ordinator and the governors in accordance with the requirements of "The Safeguarding Vulnerable Groups Act 2006", which came in to effect in 2008 and in accordance with the schools safeguarding policy. Poulner Junior School aims to promote a safe working environment for all pupils. Pupils should feel happy that they can raise any issues of concern with the relevant member of staff.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan for and make use of ICT, for example, web-based resources and e-mail. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop ICT life skills in their use. Access to the internet is a necessary tool for staff and pupils. It is an entitlement for pupils who show a responsible and mature approach towards its use.

Aims

To give pupils the opportunities to:

- Access world-wide educational resources;
- participate in new initiatives such as a managed learning environment.
- gather information and have cultural exchanges between appropriate pupils in other schools;
- provide access to educational materials and good curriculum practice;

Scope

This policy applies to all school equipment and the use thereof, at any time, and all other ICT equipment brought onto the school premises by staff (including mobile internet devices). Staff should seek the permission of a member of SLT before bringing their own equipment onto the premises.

Management

- The School Leadership Team (SLT) will delegate editorial responsibility of our school website to the School Website Manager to ensure that content is accurate and quality of presentation is maintained;
- Pupils will be made aware that the quality of their work published on the web needs to reflect the diversity of the audience;
- Photographs must not identify individual pupils in any way.
- Full names will not be used anywhere on the external website, particularly alongside photographs;
- Parents will be informed that pupils will be provided with supervised internet access;
- Personal CD's and memory sticks may not be brought into school by pupils unless authorised by an adult (e.g. for sharing home learning);
- Management of safe internet access is delegated to Hampshire County Council through their black/white list. In the case of any safeguarding issues that should arise please refer to the relevant section of the safeguarding policy which takes precedent over this policy in cases of doubt.
- Rules for internet access will be posted near computer systems. The 'Rules for Responsible Internet Use' will be printed as posters (see appendix 1);

- All staff, including teachers, supply staff, teaching assistants and support staff will be provided with the Internet Policy, and its importance explained;
- Parents' attention will be drawn to the policy in newsletters, the school brochure and on the school website and also in the Poulner School Diary/ Home communication Book which provides the children with an ICT Acceptable Use Policy.(see end of page)

Responsibility for handling breaches of this policy will be given to the SLT;

Planning and use of the Internet

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirement;
- Pupils will be given clear objectives for internet use;
- Staff will select sites which will support the learning outcomes planned for the pupils' age and maturity;
- Approved sites * must be bookmarked, listed or copied to the school intranet;
- Staff and pupils **will not** be allowed to access public chat rooms, including social network sites (except through our VLE managed and monitored by staff);
- Staff and pupils will not access inappropriate sites * that could put others at risk;
- New facilities will be thoroughly tested before pupils are given access;
- internet access will be granted to a whole class as part of the scheme of work, after a suitable education in responsible internet use;
- Pupils using the Internet will be supervised by an adult;
- If staff or pupils discover unsuitable sites, the URL (address) and content will be immediately reported to the Internet Service Provider via the ICT leader.

* Administration of White/blacklisting of websites is delegated to Hampshire County Council

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school. 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 should note that:

- 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, 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;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials must be respected;
- Censorship of inappropriate sites is maintained through the Hampshire firewall;
- All internet activity should be appropriate for staff professional activity or pupils' education plus reasonable personal use outside teaching contact time.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded or may be sent inadvertently to the wrong person:

- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Users will be aware when they are accessing inappropriate materials and should expect to have their permission to use the system removed;
- Staff should not give their email address to pupils.

Any material breach of this will result in disciplinary action.

Appendix 1

Rules for Responsible Internet Use

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

- I will only access the email with my own ID and password, which I will keep secret;
- I will not access other people's files;
- I will only use the computers for school work and homework;
- I will not bring CD's or a memory stick into school;
- I will ask permission from a member of staff before using the internet;
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and sensible;
- I will not give my home address, telephone number, email address or personal website details, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that the school may check my computer files and may monitor the internet sites I visit.

Acceptable internet use policy - Use of the internet by employees of Poulner Junior School is permitted and encouraged where such use supports the goals and objectives of the business.

However, Poulner Junior School has a policy for the use of the internet whereby employees must ensure that they:

- ☐ comply with current legislation
- ☐ use the internet in an acceptable way
- ☐ do not create unnecessary business risk to the organisation by their misuse of the internet

Unacceptable behaviour

In particular the following is deemed unacceptable use or behaviour by employees:

- ☐ visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- ☐ using the computer to perpetrate any form of fraud, or software, film or music piracy

- ❑ using the internet to send offensive or harassing material to other users
- ❑ downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- ❑ hacking into unauthorised areas
- ❑ publishing defamatory and/or knowingly false material about (organisation name], your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- ❑ revealing confidential information about Poulner Junior School in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
- ❑ undertaking deliberate activities that waste staff effort or networked resources
- ❑ introducing any form of malicious software into the corporate network

Organisation-owned information held on third-party websites

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of Poulner Junior School. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Monitoring

Poulner Junior School accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the organisation.

In addition, all of the organisation's internet-related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the organisation's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record. [These procedures will be specific to your organisation. They should reflect your normal operational and disciplinary processes. You should establish them from the outset and include them in your acceptable use policy.]

Agreement

All company employees, contractors or temporary staff who have been granted the right to use the organisation's internet access are required to sign this agreement confirming their understanding and acceptance

ICT Acceptable Use Policy



When using the school network, I will:

- ★ only access the school computer network using my own ID and Password.
- ★ ask a member of staff to remind me of my login details if I cannot remember them.
- ★ never log on using another person's details and endeavour to keep my codes secret.
- ★ always log off when I am finished on the computer.
- ★ not attempt to alter any computer settings, including background images.
- ★ always ask permission before attempting to transfer any files to the school network.
- ★ not attempt to download, upload or otherwise bring onto the school network programs and files that may contain hidden programs (zip, exe, etc.). This includes all files that may be used for purposes forbidden on the school network such as games and chat rooms.
- ★ not attempt to deliberately seek out files on the school network that may be used for malicious purposes.
- ★ never access other people's files unless a copy has been sent to me by email.
- ★ only use the computers for school work or homework.
- ★ always handle the equipment with care and respect.
- ★ report any faults to my teacher straight away.

When using the Internet, I will:

- ★ ensure a teacher is present in the room before using the Internet and always ask if I may use it, unless I have been directed to do so as part of my lesson.
- ★ not deliberately seek out inappropriate or offensive material.
- ★ not deliberately seek to bypass the school Internet filters in order to gain access to sites that have been deemed inappropriate.
- ★ report any material that I accidentally come across that is inappropriate to my teacher. This applies to any material of a violent, dangerous, racist or inappropriate sexual nature.

ICT Acceptable Use Policy



- ★ not download applications or other software.
- ★ not access games sites other than those specifically directed by my teacher for educational purposes.
- ★ never publish personal details about myself, my friends or other people that I know.
- ★ not use chatrooms or instant message type applications.
- ★ refrain from using foul language in any email correspondence and will never use the school email system to send messages that are aimed at causing harm or upset to others.
- ★ always report any unpleasant emails I am sent to a teacher.
- ★ not open email attachments without the permission of my teacher.

Acceptable Use Policy

Pupil Name: _____

Tutor Group: _____

- ★ I confirm that my son/daughter has read the attached terms of acceptable use and agrees to abide by them when using the ICT facilities available within the school.
- ★ I understand that the school may check my son/daughter's computer files and monitor the Internet sites they visit.
- ★ I understand that failing to comply with these rules may result in sanctions being applied to their account, restricting access to the facilities for a period of time - or even permanently in some instances - and this may impact their learning.

Signature (Parent): _____

Signature (Pupil): _____

