

(Not protectively marked.)



**Ham Drive Nursery School and
Day Care**

INTERNET POLICY

INTRODUCTION

Access to the Internet is important for education, business and social interaction and can make a positive contribution to lifelong learning for children and adults. Alongside the benefits of the Internet, the school recognises the potential dangers associated with its use and so has a duty to provide children and staff with a quality and safe experience.

Possible benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments;
- educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DfE.

Developing good practice in Internet use is based upon:

- designing access to the Internet access with the needs of staff and pupils in mind;
- maintaining appropriate levels of filtering material accessible from the Internet;
- guiding pupils in on-line activities that will support the learning outcomes planned for their age and maturity;
- ensuring the school complies with copyright law when using materials accessed by staff and pupils;

Ham Drive: reporting unsuitable material using the URL (address) to the South West Grid for Learning (SWGfL) via the ICT co-ordinator.

Plymouth Nursery Schools Federation.

(Not protectively marked.)

- 0870 9081708 or email: abuse@swgfl.org.uk
- **Plym Bridge:** reporting unsuitable material to the Tor Bridge High ICT team who are responsible for Internet security: 01752 207887.

E-mail

Restriction of incoming and outgoing e-mail to approved addresses and filtering for unsuitable content and viruses is now possible. This is a feature of Easy Mail+, which is used at Ham Drive Nursery School and Microsoft Outlook, used at Plym Bridge. When used in school e-mail should not be considered private and most schools and businesses reserve the right to monitor e-mail. There is a balance to be achieved between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation. Pupils at Plymouth Nursery Schools Federation will not need or have access to e-mail.

Additionally:

1. A risk assessment will be carried out before pupils are allowed to use a new technology in school.
2. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

On-line Communications and Social Networking

A number of technologies allow people to communicate other than by using; e-mail, Chat through the Microsoft service, such as Messenger allows pupils to send text messages, voice and web cam video in real time. There is also a range of newer services within the genre of Social Networking Sites that allow people to upload text, images, sound and video which can then be shared across the whole Internet, or with specific friends; examples include Facebook, Bebo and My Space.

- The ability to post personal information and communicate with friends is hugely appealing to young people, with an increasing number of Key Stage 2 pupils having accessed these services. It is a major concern how pupils use these appropriately and safely. For example; to ensure that only very limited personal information is included on a person's social networking site, not allowing them to be easily identified. All of these services and ones similar in nature are filtered by SWGfL (at HDNS) and by Tor Bridge High ICT team who are responsible for Internet security for PB.
- . These are banned from pupil access while at school, but are likely to be accessible from home. Schools have a key role to teach young people about the importance of keeping personal information safe, not posting comments and pictures of other people that may cause upset and to communicate in an appropriate manner. These issues are unlikely to be raised with the children, however whenever children are likely to be exposed to these media; e.g. when being photographed during events where parents are present, an announcement will always be made

Plymouth Nursery Schools Federation.

(Not protectively marked.)

asking all those present to respect other people's privacy by not uploading any images or video footage to the internet.

The use of social networking sites (such as Facebook, My Space etc) and chat rooms is not permitted at school.

All members of staff should also be made aware of maintaining professional codes of conduct in their own personal use of such media.

School website

- No content should be uploaded onto the school website unless it is authorised by the headteacher and does not breach copyright.
- To ensure the privacy and security of staff and children, the contact details on the website should be the school address, email and telephone number only.
- Children's full names will never be published on the website.

Links to external websites will be regularly reviewed to ensure that their content is appropriate.

Internet Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. It should be clear who has Internet access and who has not and parental permission will be required in all cases.

1. All staff must accept the terms of the 'Responsible Internet Use' statement (below) before using any Internet resource in school. Discretion and professional conduct is essential.
2. The school will keep a record of all staff and pupils who are granted Internet access;
3. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn;
4. Within the school access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials;
5. Parents will be informed that pupils will be provided with supervised Internet access;
6. Parents will be asked to sign and return a consent form;

Risk Assessment

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. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Plymouth Nursery Schools Federation.

(Not protectively marked.)

- Methods to identify, assess and minimise risks will be reviewed regularly.

The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Filter Management

Internet access must be appropriate for all members of the school community from youngest pupil to staff. Levels of supervision will vary according to the pupil's age and experience.

The LA in conjunction with the SWGfL has implemented Safety Net+. This service filters Internet access by cross referencing all web site requests against a banned list which is continually updated. In addition to this schools can permit or deny sites that they feel appropriate for the duration they choose, at Plym Bridge this is provided by Tor Bridge High ICT team who are responsible for Internet security.

However, despite careful design, filtering systems cannot be completely effective due to the speed of change of web content.

Careful monitoring and management of the Internet filtering system will still be required, i.e. checking to ensure that staff are aware of this service and being proactive in its use.

It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

1. The school will work in partnership with parents, the DfE, the LA and the SWGfL and Tor Bridge ICT team to ensure systems to protect pupils are reviewed and continually updated.
2. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
3. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
4. Any material that the school believes is illegal must be referred to the Internet Watch Foundation (please see references given later).
5. Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

This policy has been developed by the Governors and the Headteacher in accordance with relevant guidance materials (some of which are accessible below) and has been agreed with staff at the appropriate level.

This policy document will be reviewed by the Governing Body on an annual basis to ensure it is up to date with current legislation and best practice.

Plymouth Nursery Schools Federation.

(Not protectively marked.)

Responding to Incidents:

- All incidents and complaints relating to internet safety use must be reported to the head teacher.
- Where incidents or complaints relate to a member of staff, the matter must always be reported to the headteacher for action.
- Incidents involving the headteacher must be reported to the chair of governors.
- The headteacher should keep a log of all incidents and complaints and regularly review the information/ evidence of emerging patterns of behaviour or weaknesses in the school's policy.
- Staff witnessing the misuse of ICT by a colleague should report this matter to the headteacher immediately.
- The headteacher will take the necessary disciplinary action and report the matter to the governors and police where appropriate.

Date reviewed and re-adopted: 19th April 2018

Signed: (Chair of Governors).

Name:

Policy Review Cycle: Three yearly. Date to be reviewed: April 2021.

Plymouth Nursery Schools Federation.

(Not protectively marked.)

Appendix One:

Letter to parents

Responsible Internet Use Statement

As part of children's educational entitlement Ham Drive Nursery School and Day Care/Plym Bridge Nursery School and Day Care is providing supervised access to the Internet. We believe that the safe, enjoyable and educational use of this resource is a worthwhile skill for young children to acquire.

Although there are concerns about children having access to undesirable materials, we have taken positive steps to reduce 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 we can provide references to information on safe Internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst we try to ensure that suitable restrictions are placed on access to 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 however it will ensure that:

- All staff are required to accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school;
- All staff (including teachers, supply staff, classroom assistants and support staff) will be provided with the School Internet Policy, and its importance explained;
- Staff should be aware that Internet traffic is monitored and reported by the SWGfL and can be traced to the individual user;
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

Maintaining ICT Security

- The school ICT systems will be reviewed regularly with regard to security and virus protection will be installed and updated regularly, daily if possible (this can be achieved by using the self updating feature within Sophos);
- Security strategies will be discussed with the LA, particularly where a wide area wireless network connection is being planned;
- Personal data sent over the Internet will be encrypted or otherwise secured;
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed;
- Portable media may not be brought into school without specific permission and a virus check;

Plymouth Nursery Schools Federation.

(Not protectively marked.)

- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked;
- The ICT co-ordinator manager will monitor the Internet usage and associated traffic in order to assess whether the capacity of the Internet is being reached.

Please would you sign and return the consent form to the school administrator so that your child may use the Internet at school. However, should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone the school and arrange an appointment with the Headteacher.

CONSENT FORM

Children may as part of their educational provision access suitable internet sites in line with the above statement. If you agree to your child having access to partake in this activity please sign the statement below.

I..... parent/carer ofgive permission for him/her to access the internet at Ham Drive Nursery School and Day Care/Plym Bridge Nursery School and Day Care as outlined above.

Signed:

Date:

Plymouth Nursery Schools Federation.

(Not protectively marked.)

Appendix Two:

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials 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 unauthorised or unlawful text, imagery or sound.

SWGfL - (including the registering of inappropriate content needing to be filtered)

Telephone: 0870 9081708

Email: support@swgfl.org.uk to notify of an inappropriate web site: abuse@swgfl.org.uk

Useful References

National Action for Children (NCH)

www.nchafc.org.uk/itok

Parents Guide on Internet usage

Bullying Online

www.bullying.co.uk

Advice for children, parents and schools

Parents Online

www.parentsonline.gov.uk/2003/parents/safety/index.html

Interactive learning and safety advice, excellent presentation for parents

Kidsmart

www.kidsmart.org.uk

An Internet safety site from Childnet, with low-cost leaflets for parents

Family Guide Book (DfES recommended)

www.familyguidebook.com

Information for parents, teachers and pupils

NCH Action for Children

www.nchafc.org.uk

Expert advice for children, young people and parents

Safekids

www.safekids.com

Family guide to making Internet safe, fun and productive

Plymouth Nursery Schools Federation.

(Not protectively marked.)

NAACE / BCS

www.naace.org

A guide for schools prepared by the BCS Schools Committee and the National Association of Advisers for Computer Education (NAACE)

DfE Superhighway Safety

www.teach-ict.com

Good reading on both Internet or by Telephone: 0845 6022260

Internet Watch Foundation -

www.iwf.org.uk

Invites users to report illegal websites

Data Protection

www.informationcommissioner.gov.uk

New Web site from the Information Commissioner

DotSafe – European Internet Safety Project

<http://dotsafe.eun.org>

A comprehensive site with a wide range of ideas and resources