Pegswood Primary School

E-Safety Policy

November 2016

CONTENTS

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and touch screen tablet devices. Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

Young people have access to the Internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe internet use by pupils not only in school, but also while on-line at home or elsewhere.

1. Core Principles of Internet Safety

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones.

There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

2. Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems.

3. How will Internet use enhance learning?

The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.

Pupils will learn appropriate Internet use and be given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4. How will Internet access be authorised?

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.

Parents will be informed that pupils will be provided with supervised Internet access.

5. How will filtering be managed?

The school will work in partnership with parents; the Local Authority and PCE (Policy Central Enterprise) to ensure systems to protect pupils are reviewed and improved.

Use of mobile devices will be monitored and tracked by "Lightspeed" – a Local Authority tracking system. All children and staff will log on to mobile devices with a personal log in so that usage can be monitored affectively.

If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the ICT co-ordinator or Head Teacher. Parents of the children involved will be notified immediately.

ICT co-ordinator and Head Teacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

6. 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. 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.

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

The Head Teacher and ICT co-ordinator will ensure that the Internet policy is implemented and compliance with the policy monitored.

7. Managing Content

7.1 How will pupils learn to evaluate Internet content?

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Coordinator/Head Teacher.

Schools should ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.

Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.

Nominated persons (ICT Coordinator/Head Teacher) will be responsible for permitting and denying additional websites as requested by colleagues.

7.2 How should website content be managed?

The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

8. Communication

8.1 Managing e-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive an offensive e-mail.

Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

Whole-class or group e-mail addresses should be used.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

8.2 On-line communications and social networking

Safe use of Social Network sites will be taught as part of the computing curriculum.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for Primary aged pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites as part of the e safety programme.

8.3 Mobile technologies

Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.

Pupils may bring mobile phones into school in Year 5 and Year 6 (Year 4 from the summer term if they are walking home unaccompanied). The phones must be locked away in the pupils' lockers and are not allowed to be used during the school day. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

9. Introducing the Policy to Pupils

Rules for Internet access will be posted in all rooms where computers are used.

A unit of work on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.

Instruction on responsible and safe use should precede Internet access.

Pupils will be informed that Internet use will be monitored.

10. Parents and E-Safety

Parents' attention will be drawn to the School E-Safety Policy and it will be posted on the school Website.

Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.

Internet issues will be handled sensitively to inform parents without undue alarm.

A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

All parents will receive support information as and when available.

11. Consulting with Staff and their inclusion in the E-safety Policy

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.

The school's consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.

All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

Community users of the school's ICT facilities must sign the acceptable user policy before being granted access.

Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

12. How will complaints be handled?

Responsibility for handling incidents will be delegated to the Head Teacher.

Any complaint about staff misuse must be referred to the Head Teacher.

Pupils and parents will be informed of the complaints procedure.

Parents and pupils will need to work in partnership with staff to resolve issues.

There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Laptop/Ipad policy for Pegswood Primary School staff (Autumn 2016)

1. The laptop/Ipad remains the property of Pegswood Primary School.
2. The laptop/Ipad is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Pegswood Primary School Staff should use the laptop/Ipad.
3. On the teacher leaving the school's employment, the laptop/Ipad is returned to Pegswood Primary School.
4. Staff on extended leave of 4 weeks and over should return their laptop/Ipad to the school (other than by prior agreement with the Head Teacher).
6. Whenever possible, the laptop/Ipad, when taken out of school, must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
7. The laptop/Ipad must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Head Teacher with evidence of adequate insurance.
8. Staff may load their own software onto the laptop/Ipad but it must be fully licensed and not corrupt any software or systems already installed on the laptop/Ipad.
9. Any software loaded must not affect the integrity of the school network.
10. If any removable media is used then it must be checked to ensure it is free from any viruses.
12. If any fault occurs with the laptop/Ipad, it should be referred to Dave Adams (Computer Technician)
13. The laptop/Ipad would be covered by normal household insurance. If not it should be kept in school overnight.

Name..

Signature: ....

Date: November 2016

Policy for responsible e-mail, network and Internet use for Pegswood Primary School.

1. I will use all ICT equipment issued to me in an appropriate way. I will not:

- Access offensive website or download offensive material.
- Make excessive personal use of the Internet or e-mail.
- Copy information from the Internet that is copyright or without the owner's permission.
- Place inappropriate material onto the Internet.
- Will not send e-mails that are offensive or otherwise inappropriate.
- Disregarded my responsibilities for security and confidentiality.
- Download files that will adversely affect the security of the computer and school network.
- Access the files of others or attempt to alter the computer settings.
- Update web pages etc. or use pictures or text that can identify the school, without the permission of the Head Teacher.
- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Pegswood Primary School.

2. I will only access the system with my own name and registered password, which I will keep secret.

3. I will inform the ICT School's Technician as soon as possible if I know my password is no longer secret.

4. I will always log off the system when I have finished working. ·

5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.

6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Head Teacher and register the passwords with the Head Teacher.

7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.

8. I will not open e-mail attachments unless they come from a recognised and reputable source.

9. I will bring any other attachments to the attention of the ICT technician, (Dave Adams.)

10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
11. I will report immediately to the Head Teacher any unpleasant material or messages sent to me.
12. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
14. Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.
15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop/Ipad removed and that other disciplinary consequences may follow.

Name..

Signature: ....

Date: November 2016

Notes on the Legal Framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place. Schools could start by banning private use of a school's computer system, but then allow private use following the signing of an agreement to use the equipment under the conditions as laid out by the school. (A copy of the Council's policy is included in section 15). The Rules for Responsible Internet Use, to which every user must agree, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights

Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. For example, each school can review the websites visited by the school each day / week / month. Though this is not user specific it does allow a degree of monitoring to be conducted. All schools are also able to monitor school e-mail.

Cyber-stalking & Harassment

(http://wiredsafety.org/gb/stalking/index.html)

Under Section 1 of the Malicious Communications Act 1998 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening. In both cases the offence is punishable with up to six months' imprisonment and/or a fine of up to £5000. As the Malicious Communications Offence is more wide-ranging than the Telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence. In most cases involving malicious communications or cyber-stalking however there will be more than one offensive or threatening letter or telephone call and therefore the police will often choose to charge the offender with an offence contrary to Section 2 of the Protection from Harassment Act 1997; also punishable with up to six months' imprisonment. Part of the reason for using this charge is that when someone is convicted of an offence under the Protection from Harassment Act 1997 the court can make a Restraining Order preventing them from contacting their victim again. Breach of a Restraining Order is punishable with up to five years' imprisonment. A Restraining Order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the e-mails, cyber-stalking etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to Section 4 of the Protection from Harassment Act 1997 which is punishable with up to five years' imprisonment and also allows the court to make a Restraining Order.

If the e-mails, cyber-stalking etc. is racist in nature or motivated by religious hostility then charges could be brought of Racially or Religiously-Aggravated Harassment contrary to Sections 32(1)(a) or

32(1)(b) of the Crime and Disorder Act 1998. If convicted offenders could face up to7 years' imprisonment.

The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In those circumstances the victim could consider taking out an Injunction under Section 3 of the Protection from Harassment Act 1997. However we would always advise informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions victims of harassment can sue the offender under Section 3 of the Protection from Harassment Act 1997 for damages arising out of the anxiety caused by the harassment and any financial loss it caused.

15. Glossary of Terms

Blog – Short for Web Log, an online diary

Podcast – a downloadable sound-recording that can be played on computers and MP3 players

Social Networking – websites that allow people to have "pages" that allow them to share pictures, video and sound and information about themselves with online friends.

Video Blogging – online videos that can be uploaded via a web cam

Web 2 Technologies – a collection of online web services that are based around communicating/sharing information