Newton Tony School

E-Safety Policy

The E-Safety Policy was reviewed in April 2013
It should be read in conjunction with the Aims of the School, Home School Agreement, the Handbook (for staff, supply and volunteers), the Complaints Policy, the Abuse and Use of ICT Policy, the Anti-bullying Policy, the Sex and Relationship Education Policy and the Health and Safety Policy with its related policies.
This policy will be reviewed in 2014

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory 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 email and mobile learning, such as phones. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

1. Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and well-being, to support the professional work of staff and to enhance the school's management information and administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

2. How will Internet use enhance learning?

- The school Internet access is designed expressly for educational use and includes filtering appropriate to the age of pupils.
- Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3. How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access, i.e. through the Responsible Use agreement for pupils and the staff policy for Responsible e-mail, Network and Internet Use.
- Primary pupils' home-school agreement includes the acceptable use policy and guidance for video, sound and images for web publication. (See appendix 15).
- Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- Parents are informed that pupils will be provided with supervised Internet access.

4. How will filtering be managed?

- A designated member of staff will manage the permitting and banning of additional web sites identified by the school.
- The school will work in partnership with parents, Wiltshire Council, DCFS and the SWGfL 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 the Internet Service Provider (SWGfL) via the ICT co-ordinator.
- Website logs will be regularly sampled and monitored through the SWGfL monitoring service: (http://monitoring.swgfl.ork.uk).
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (IWF - http://www.iwf.org.uk/).

5. 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 Wiltshire Council 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 Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

6. Managing content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the South West Grid for Learning: 0845 307 7870 or email: abuse@swgfl.org.uk
- Specific lessons will be included within the curriculum that teaches all pupils how to develop their media literacy skills, in particular validity and bias.
- At Key Stage 2, Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Training should be available to staff in the evaluation of web materials and methods of developing students' critical attitudes.

6.1 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.

7. Communication

7.1 Managing e-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mails.
- Pupils must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Whole-class or group e-mail addresses should be used at Key Stage 1 & 2.
- Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.
- Access in school to external personal e-mail accounts is not allowed.
- 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.

7.2 On-line communications and social networking.

- The school will conduct regular pupil surveys (three-yearly or ideally more often) about home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
- The use of online chat is not permitted in school, other than as part of its online learning environment.

7.3 Mobile technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are not permitted within the school. Pupils/students will be asked to give them to their teacher/tutor at the start of the school day.

8.Introducing the Policy to Pupils

- Rules for Internet access will be posted in all rooms where computers are used.
- Instruction on responsible and safe use should precede Internet access.
- Pupils will be informed that Internet use will be monitored.
- The teaching of e-safety will be part of the curriculum for all pupils.

9. Parents and E-Safety

- Parents' attention will be drawn to the school e-Safety policy in newsletters, the school brochure and 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.
- A partnership approach with parents will be encouraged. This could include parent's evening, school newsletter, practical sessions and suggestions for safe Internet use at home.

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as Childnet International, PIN, Parents Online and NCH Action for Children.

10. Consulting with staff and their inclusion in the e-safety policy

- All staff including teachers, supply staff, classroom assistants and support staff, will be asked to sign the Policy for responsible e-mail, network and Internet use.
- 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.
- Staff should be aware that Internet traffic is monitored and reported by the SWGfL and can be traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
- 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.

11. How will complaints 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 Headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - informing parents or carers.
  - removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system.

This policy was agreed by the Governing Body:

SIGNED ……………………………………………….. ………………………………………………………………………….

Chair of Governors **Headteacher**

DATE: 18th April, 2013

Newton Tony Primary School

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

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. The South West Grid for Learning (SWGfL) monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

Newton Tony Primary School

Letter to Parents

1 September 2012

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Newton

Tony Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, the South West Grid for Learning (SWGfL) operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access 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.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone me to arrange an appointment.

Yours sincerely

GM Clark
Headteacher

Newton Tony Primary School

Responsible Internet Use

Please complete, sign and return to the school secretary

Pupil: **Class:**

Pupil's Agreement

I have read and I understand the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed: **Date:**

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: **Date:**

Please print name:

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school Website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that this content will not clearly identify individuals and that full names will not be used.

Signed: **Date:**

Laptop policy for Newton Tony Primary School staff 2012 – linked to IWB.

1. The laptop remains the property of Newton Tony School.
2. The laptop 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

   Newton Tony School Staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Newton Tony School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the headteacher).
4. When in school and not being used, the laptop must be switched off and kept secure.
5. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
7. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
8. Any software loaded must not affect the integrity of the school network.
9. If any removable media is used then it must be checked to ensure it is free from any viruses.
10. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up to date.
11. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
12. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
13. Students must never use the laptop.
14. If any fault occurs with the laptop, it should be referred immediately to the Network Manager.
15. When being transported, the carrying case supplied must be used at all times.
16. The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

Policy for responsible e-mail, network and Internet use Newton Tony 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.
   - Disregard my responsibilities for security and confidentiality.
   - Download files that will adversely affect the security of the laptop 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 headteacher.
   - Attempt to repair or interfere with the components, software or peripherals of any

     computer that is the property of Newton Tony School.
2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will always log off the system when I have finished working.
4. 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.

5. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Headteacher and register the passwords with the Headteacher.
6. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
7. I will always adhere to the Newton Tony School Software Compliance Policy.
8. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager.
9. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
10. I will report immediately to the Headteacher any unpleasant material or messages sent to me.
11. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
12. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
13. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.
14. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
15. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name……………………………………………………

Signature: ……………………………………………

Date: …………………………………………………

Glossary of Terms

Blog – Short for Web Log, an online diary

DCSF - Department for Children, Schools and Families

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

SWGfL – South West Grid for Learning, which provides Internet access and associated managed services to all schools in the South West

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

Web-based Resources

For Schools

KidSmart http://www.kidsmart.org.uk/
SMART rules from Childnet International and Know It All for Parents

Childnet International http://www.childnet-int.org/
Guidance for parents, schools and pupils

Becta http://schools.becta.org.uk/index.php?section=is
e-Safety Advice

Becta / Grid Club, Internet Proficiency Scheme
On-line activities for Key Stage 2 pupils to teach e-safety.
http://www.gridclub.com/teachers/t_internet_safety.html

Kent Local Authority http://www.clusterweb.org.uk/kcn/e-safety_home.cfm
Additional e-safety materials (posters, guidance etc.)

London Grid for Learning http://www.lgfl.net/lgfl/sections/safety/esafety/menu/
Additional e-safety materials (posters, guidance etc.)

DfES Anti-Bullying Advice http://www.dfes.gov.uk/bullying/

Grid Club http://www.gridclub.com/teachers/t_internet_safety.html

Internet Watch Foundation www.iwf.org.uk
Invites users to report illegal Websites

South West Grid for Learning – Safe www.swgfl.org.uk/safe
A comprehensive overview of web-based resources to support schools, parents and pupils

South West Grid for Learning – Filtering
http://www.swgfl.org.uk/services/default.asp?page=filtering

Think U Know www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Wiltshire County Council – WISENET
http://wisenet.wiltshire.gov.uk/documents/dsweb/View/Collection-922

Facebook for Educators http://www.facebook.com/fbsafety
(Linda Fogg Phillips, Derek Baird, MA & BJ Fogg Ph.D

For Parents

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

Childnet International http://www.childnet-int.org/
"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe

Useful contact details:

South West Grid for Learning (SWGfL) Support Team - (including the registering of inappropriate content needing to be filtered).

Telephone: **0870 9081708**

E-mail: **support@swgfl.org.uk**

To notify of an inappropriate website: **abuse@swgfl.org.uk**

• 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 to 7 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.