Toynton-All-Saints Primary School
E- Safety Policy

aspire | achieve | innovate

Introduction

The Learning Trust (TLT) recognises the need to maintain a strategy for effective use of the Internet as a valuable tool for learning. It also recognises the need to protect user in particular young people, from offensive and dangerous material and acknowledges the need to ensure that all users make responsible use of the Internet. This document is based on recent Government and BECTA guidelines. It updates and replaces previous guidance issued by TLT I.T. Services.

Key Points

A brief summary of the Key Points is made here for easy reference. More detailed notes are contained in the pages which follow and exemplar materials are in the Appendices.

Schools have the following responsibilities:-

 To designate a senior member of staff to be responsible for pupil safety and security policies related to the Internet and electronic communications, for example, e-mail.)
 To ensure that all internet access is supervised.
 To provide for learners, parents, staff and any other adults an Acceptable Use Policy Agreement, before being allowed Internet access.
 To have a system of immediate sanctions for dealing with improper use of ICT equipment and its use.
 To make parents aware of Internet Safety policy and procedures;
 To connect to the Internet through a filtered service.
 To ensure that staff and learners are aware that their e-mail use and Internet activity is monitored.
 To follow TLT guidelines on the use of photos and personal details on school websites. (See Appendix A)
 To follow TLT guidelines on the use of video-conferencing and/or webcams
 with/by learners
 To incorporate the misuse of mobile phones and Personal Digital Assistants (PDAs) when drafting ICT policies. (See Appendix B)
 To reinforce the understanding of staff and learners that material on the Internet is subject to copyright legislation.
 To include Internet Safety as part of the Personal and Social Development programmes.

Internet Safety Policy

aspire | achieve | innovate

Staff in schools and other education centres have the following responsibilities:

 To ensure that all Internet use by learners is **supervised**
 To implement TLT and School Policies and procedures;
 To ensure that people in their care understand and follow policy and procedures;

Learners in education centres have the following responsibilities:

 To have a responsible attitude to the use of, school ICT equipment and internet / email provision
 To follow the Schools Policies on Acceptable Use
 To follow the ‘Net Rules’ guidance

THE FOLLOWING ACTIVITIES ARE STRICTLY PROHIBITED:

 Use of the Internet to harass, offend or bully any other person;
 Use of the Internet for any inappropriate or illegal purpose;
 Use of the Internet for transmission or reception of threatening or obscene

material;
 Use of the Internet for transmission or reception of material from any criminal organisation;
 Use of the Internet for the transmission or reception of viruses or unlicensed software;
 Use of the Internet for any personal, commercial purpose or profit.
 The 'Use of the Internet' also implies the use of personal devices or other internet capable mobile communication devices in schools.

Internet Safety Policy

aspire | achieve | innovate

The following points are expanded below:

Appendix A Acceptable Use Agreement

Appendix B Internet Rules

Appendix C Exemplar School Policy

Appendix D Use of Photos

Internet Safety Policy

aspire | achieve | innovate

1 Responsibility

The school should designate a senior member of staff as responsible for student
safety and security policies related to the Internet and electronic communications.

The designated person along with the Network Administrator/ICT Manager should ensure that policies are implemented and that regular monitoring takes place. All staff, including temporary and student teachers, should be made aware of school and Learning Trust (TLT) policies. Schools which offer Internet access to members of the public out with school hours, such as adults on Community Learning courses, should take measures to ensure that this access in no way compromises student use and

safety.
All users should be encouraged to use computers and the Internet responsibly and to understand the consequences with their actions could have on themselves and others.

2 Supervision

Learners should never be left unsupervised when using the Internet.
The key to ensuring online safety is to supervise all Internet use. Computers should be within sight of the teacher, not tucked away in a corner where it is difficult to see what a student is doing. For senior pupils in secondary schools (mature students), the teacher, or responsible adult, may be supervising indirectly, but still be aware of learners' access and monitoring their use.
When direct supervision by school staff is not possible, those with responsibility for the learners should be informed of the TLT's policies on Internet Safety. For example, employers who have learners on work placement schemes should not allow them to have unsupervised unfiltered Internet access.
When parents/carers enroll children the School must ask parents to "give consent to their son/daughter having Internet access in a supervised situation", but parents have the right to withdraw their permission at any time

3 Acceptable Use Policy (AUP)

Learners, parents/carers, staff and any other adults with Internet access must sign
an Acceptable Use Policy Agreement.
Such and agreement makes everyone aware of their responsibilities when using the Internet. Younger children, who will not understand the AUP, should not be expected to sign but parents/carers need to know what is expected of their children and to give permission for their children to use the Internet. Parental permission only has to be given once for the whole of a child's stay in one school but parents have the right to withdraw their permission at any time.
An exemplar AUP can be found in the appendix.
(Appendix A Acceptable Use Agreement)

Internet Safety Policy

aspire | achieve | innovate

The rules for computer and Internet use detailed in the AUP should be displayed next to all computers.
(Appendix B Net Rules)

4 Use of the Internet

The Internet can be a rich educational resource, providing access to millions of pages of information. However, much of the Internet is unorganised and unregulated and many sites contain information, which is inaccurate, dangerous, illegal or pornographic.
Schools must ensure that learners do not have bad experiences when using the Internet or other forms of electronic communication and that parents have confidence that schools are using 'all due diligence' to protect their children. Above all, we want to avoid users being exposed to offensive materials – pornographic, violent, or racist.

Child Protection

The most serious risk to learners involves the possibility of someone being hurt, exploited or abused as a result of personal information being posted online. Online pictures, names, addresses, or age can be used to trace, contact and meet a student with the intention of causing harm.
Appropriate Child Protection Policy must be followed in instances where unacceptable use has raised child protection issues, so that the effective action can be taken.
The potential dangers should not deter teachers and tutors from allowing learners to use the Internet as the educational advantages far outweigh the disadvantages.

By following some simple guidelines and using common sense, teachers and tutors can ensure that learners can work safely online.

The following internet procedures must be followed by all users to ensure safe and responsible use of the web.

It should always be remembered that visits to sites are recorded and can be traced back to the user.

 Inform the person in charge, or TLT I.T. Services immediately if any abusive, threatening or offensive sites are discovered.

 Young children should be restricted to specific approved sites and should not use search engines (unless they have been designed for educational use).

 Care should be taken that any material published to the web does not breach any of the guidelines in this policy or other policies relating to data protection, copyright and Intellectual Property Rights (IPR).

 Personal information should never be divulged.

 Use of an adult's credit card details should not take place on education premises.

5 Use of E-mail

The following procedures must be followed by all users to ensure safe and responsible use of e-mail.

It should be remembered that e-mails are recorded, can be traced back to the sender and can be legally binding.

 Conceal access passwords and change the passwords regularly. (For practical reasons, special log-on arrangements can be made for younger children.)

 Inform the teacher, centre or TLT I.T. Services immediately if any abusive, threatening or offensive e-mails are received.

 Inform the teacher, centre or TLT I.T. Services immediately if an e-mail or attachment generates a virus warning.

Staff Use of e-mail

Staff may make personal use of the school Internet and e-mail facilities outside the normal teaching day.

Personal use is subject to the same rules that apply at other times.

 Staff should be aware that their e-mail is filtered and no school e-mail accounts are private.

 The contents of student or staff e-mail accounts or details of online activity may be checked at any time.

 Staff should never use school Internet and e-mail to send private confidential information or provide credit card details.

 Staff should be aware that their e-mail use and internet activity is monitored.

See also Appendix C

Teachers should ensure that :-

They do not engage in private/personal correspondence or communication with a student or pupil. (This includes texting and Media messaging e.g. MSN Messenger.)

They take care in communicating with learners/ learners via e-mail, especially where this involves personal or private e-mail addresses.

6 Use of Instant Messaging - MSN Messaging, Yahoo Messenger

Many pupils use this extensively at home and are very familiar with this method of making instant communication with their friends. If and when learners are using this in school, the same 'Net Rules' apply.

Internet Safety Policy

aspire | achieve | innovate

7 Data Protection

Personal information about other users should never be revealed over the Internet.

8 Virus Protection

All computers used for access to the Internet must have anti-virus software installed. This software must be regularly updated to take account of the ever growing number of viruses. Introducing viruses to computers, or attempting to break through network security is a serious offence, and schools should be aware of the issues and the risks.

Any user who suspects the presence of a computer virus must alert the Network
Administrator or other responsible person immediately!

Further general information on virus protection can be found at:
http://www.ictadvice.org.uk/

9 Copyright

Copyright rules apply to material available over the Internet. Many sites carry copyright notices indicating how the material may be used and how to obtain permission.

The following information gives basic guidelines:

- *Always acknowledge sources*
- *Never assume that educational use of material is permitted, without first checking with the author*
- *Staff and learners should be aware that work published on websites may be open to unauthorised use*
- *Publishing other people's material without their explicit permission is a breach of copyright: This would certainly apply to use of images, jpegs etc on a school website*
- *Using a website live or from a cache in a lesson is not a breach of copyright, but copying an entire page into, for instance, a PowerPoint presentation would be*
- *Copying material from the Internet and printing it for pupil use could be a breach of copyright: using it as part of a larger document certainly would be.*

10 Misuse of equipment

School should have a system of immediate sanctions for dealing with improper use of ICT equipment and its use. These could include:- withdrawal of access to equipment, and loss of internet privileges.

Internet Safety Policy

aspire | achieve | innovate

11 Child Protection

Child Protection is a serious issue and any serious incidents, which cause concern, must be dealt with in line with local appropriate Child Protection policies. Any incidents should be recorded by the designated person with responsibility for Internet Safety and appropriate action taken. Schools should be aware that serious incidents could lead to legal action so accurate recording and preservation of evidence is essential.

12 Informing Parents

A copy of the school's Acceptable Use Policy should be part of the School Handbook.

It is anticipated that schools may also wish to bring the existence of this 'Internet Safety' document to parents' attention, by providing a link to it in their School Handbook.

13 Mobile Phones

Mobile phones and PDAs (Personal Digital Assistants) now have similar capabilities to e-mail in that they can be used to send and receive text and pictures. Mobile phones can be used to harass or defame others so schools should consider the consequences of the misuse of mobile phones and PDAs when drafting policies on the use of mobile technology.

14 Website Development

A school web site represents the school electronically in the wider world. It should contain appropriate materials that reflect the aims and ethos of the school. Schools can provide up to date information about activities to learners, parents, the community and the wider world. However, serious concerns have been expressed as to how this information might be used by certain members of society.

Clearly, schools and other organisations have a responsibility to protect the young people in their care and should consider the risks involved in any information which appears in school websites. 'Introduction to copyright issues for websites'. This BECTA document is intended to provide website owners with a brief introduction to copyright and a summary of the main issues that need to be considered when developing a website.

15 Digital Imaging

There is a form relating to parental consent being required for the use of pupils' images in photos or digital videos. This consent is sufficient and covers legal obligations.

It should be noted, however, that this is for 'Educational Use' of these images only. Common sense suggests that where a school may wish to feature certain pupils very

Internet Safety Policy

aspire | achieve | innovate

THIS POLICY ESTABLISHED AND APPROVED FOR IMPLEMENTATION BY THE FULL GOVERNING BODY

Signed ……. (Head Teacher)

Signed ……. (Designated Governor)

Dated: ……..

The name of our appointed Designated Governor is : LIZ EVANS

The name of our School's Designated Teacher is : LESLEY COULTHURST

THIS POLICY WILL BE REVIEWED ANNUALLY ON : 21st September