



Education and Lifelong Learning
A Policy for the Safe Use of Internet Technology
Approved 29 January 2008

1. Purpose of the Policy

This policy provides guidance to headteachers and other managers in Education and Lifelong Learning (ELL) on the Safe Use of Internet Technology with learners in schools and other ELL centres. It replaces 'A Policy and Guidelines for Safe Use of the Internet in Education' published in 2001 (reviewed 2004).

2. Corporate Context

This policy should be read in conjunction with the following SBC Corporate Policies:

- Policy and Guidelines on E-mail and the Internet
- Computer Security Policy and Standards
- Data Protection Code of Practice

3. Accessibility Statement

This policy can be made available in large print, on tape or in other languages. Please call the Education and Lifelong Learning Communications Unit for advice on 01835 826592.

4. Background

Scottish Borders Council (SBC) Department of Education and Lifelong Learning 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 users, 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 Scottish Executive guidelines. It updates and replaces previous guidance issued by the SBC Information Communications Technology Unit.

The policy applies to all establishments within Education and Lifelong Learning who provide services to children and adults. The word 'learners' applies to all pupils, students and adult learners. The policy covers all technologies which access the Internet including Personal Digital Assistants (PDAs) and mobile phones. The public use of computers and the internet in libraries is covered in a separate policy ([Appendix J](#)). This policy recognises that there are differences in the needs and range of customers using computers and the internet in Libraries.

Since the publication in 2001 of the SBC 'A Policy and Guidelines for Safe Use of the Internet in Education', there have been a number of developments in:

- applications
- local area networks
- modes of communication
- volume of electronic communication
- speed of access
- availability of access
- the ability to use the Internet from a variety of mobile devices.

All of these have changed the nature and significance of the internet and other electronic communications. In SBC many of these issues have been addressed by implementing appropriate access and security policies and technical solutions at education authority and school level. The forthcoming national Scottish Schools Digital Network (Glow) project will also assist in this regard through making available to schools an environment that facilitates controlled and managed access to the internet. There remains, however, a local requirement to manage services and the policies surrounding these on an ongoing basis.

The range of Information and Communication Technology (ICT) is both increasing and converging. Establishment policies and practice should aim to take account of the ability to communicate in a wide range of ways including:

- networked computers
- palmtop and handheld computing devices
- devices connected through wireless networks
- tablet PCs
- mobile phones

Associated with this range of technologies is a range of communication applications, including the World Wide Web, file sharing (i.e. web-based file sharing utilities), internet newsgroups, videoconferencing, video streaming, email, internet chat, messaging services, digital imaging and more. Any establishment policy will have to take account of those applications which an establishment chooses to support. This is an area that is constantly changing, and sources of information need to be up to date.

5 Responsibility

All organisations should designate a senior member of staff to be responsible for student safety and security policies related to the Internet and electronic communications.

The designated person should ensure that policies are implemented and that regular monitoring takes place. All staff, including temporary, students or trainees, should be made aware of policies.

All users should be encouraged to use computers and the internet responsibly and

to understand the consequences their actions could have on themselves and others.

SBC Department of Education and Lifelong Learning has the following responsibilities:

- To ensure that clear policy guidelines are formulated and distributed to all members of staff.
- To monitor the implementation and regularly review the content of the policy to take account of developing technology.
- To identify and install suitable content filtering and audit software where Internet access is provided, in addition to any filtering service offered by the Internet Service Provider (ISP).
- To provide guidance for all staff who will be responsible for the delivery or supervision of internet based learning.
- To put in place mechanisms for monitoring responsible ICT use in establishments.

Headteachers 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.
- To ensure that all internet access is **supervised**.
- To provide for learners, parents, staff and any other adults an Acceptable Use Policy Agreement, where they must confirm acceptance of its terms, before being allowed Internet access.
- To have a system of immediate sanctions for dealing with improper use of ICT equipment as part of the school's behaviour management policy.
- To make parents aware of Internet Safety policy and procedures.
- To connect to the Internet only through the filtered network service.
- To ensure that staff and learners are aware that their e-mail use and Internet activity is monitored.
- To follow SBC policy on the use of photos and personal details on school websites.
- To follow SBC policy 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.
- To reinforce the understanding of staff and learners that material on the Internet is also subject to copyright legislation.
- To include Internet Safety as part of the Personal and Social Development programmes.
- To review existing policies including behaviour management and anti-bullying policies to reflect the threat of technology abuse.

Managers in other Education and Lifelong Learning centres have the

following responsibilities:

- To ensure that all Internet use by learners is monitored.
- To implement SBC and ELL Policies and procedures in relation to Internet technologies.
- To ensure that learners understand and follow policy and procedures;
- To designate a senior member of staff to be responsible for learner safety and security policies related to the Internet and electronic communications, for example, e-mail.
- To provide for learners, staff and any other adults an Acceptable Use Policy Agreement, where they must confirm acceptance of its terms, before being allowed Internet access.
- To have a system of immediate sanctions for dealing with improper use of ICT equipment.
- To connect to the Internet only through the filtered network service.
- To ensure that staff and learners are aware that their e-mail use and Internet activity is monitored.
- To follow SBC policy on the use of photos and personal details on websites. (See Appendix A)
- To follow SBC policy 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.
- To reinforce the understanding of staff and learners that material on the Internet is also subject to copyright legislation.
- To include Internet Safety as part of the Personal and Social Development programmes. (Does not apply to Libraries.)

Learners in Education centres have the following responsibilities:

- To have a responsible attitude to the use of ICT equipment and internet / email provision
- To follow Policies and Guidelines on acceptable use.
- To follow the 'Net Rules'. (Appendix E)

THE FOLLOWING ACTIVITIES ARE STRICTLY PROHIBITED ON ANY SITE:

- 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 of threatening, offensive or obscene material;
- Use of the Internet for transmission of material from any criminal organisation;
- Use of the Internet for the transmission of viruses or unlicensed software;

6 Supervision in Schools

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 or tutor, not tucked away in a corner where it is difficult to see what a student is doing. For senior pupils in secondary schools (S5 and S6) and mature students, the teacher, tutor, 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 local authority'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 at an SBC school, the SBC School Admission Form asks 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.

7 Acceptable Use Policies

Learners, parents/carers, staff and any other adults with Internet access must sign an Acceptable Use Policy Agreement.

Such an agreement makes everyone aware of their responsibilities when using the Internet. Younger children (perhaps P1-P3), who will not understand the Agreement, 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. Exemplar Agreements can be found in the appendices. 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. (Appendix C Acceptable Use Agreement)

The rules for computer and Internet use should be displayed next to all computers. (Appendix D Net Rules)

8 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 unstructured 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.

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. Scottish Borders Inter-Agency Child Protection Policy must be followed in instances where unacceptable use has raised child protection issues, so that the appropriate 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 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 in schools.

More detailed information regarding intellectual property can be found on the Learning & Teaching Scotland site: [Student's Guide to Intellectual Property: a Teaching Resource Pack](#). This pack contains everything required to start teaching pupils about Intellectual Property (IP). It includes a curriculum map, worksheets, activities, answers and a glossary.

9 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 Headteacher or Centre Manager immediately if any abusive, threatening or offensive e-mails are received.
- Inform the appropriate Help Desk immediately if an e-mail or attachment generates a virus warning.

10 Staff Use of E-mail

Staff may make personal use of the school (curricular) 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 and recorded.

The General Teaching Council for Scotland have additional general guidance for teachers. See [Appendix G](#).

Staff working with young people should ensure that:

- They do not engage in private/personal correspondence or communication with a student or pupil. (This includes texting and Media Messaging eg MSN Messenger.)
- They take care in communicating with learners via e-mail, and only use a student or pupil's education e-mail address for this purpose.

11 Use of Internet Newsgroups

Internet newsgroups can be a valuable means of exchanging information on specific topics. Some newsgroups have been developed specifically for educational purposes and are moderated to filter out any inappropriate material. Newsgroups which are not moderated are totally inappropriate for educational purposes and should not be used.

12 Using File Transfer Protocol (FTP) for downloading software

These sites allow users to download software such as drivers and application software. Because of the danger of transmission of viruses or corrupted data, such activities are restricted to the Network Administrator except where there is a curricular requirement for learners to gain experience of FTP (e.g. Higher Computing).

13 Use of Internet Relay Chat (IRC)

IRC allows users to speak to other users anywhere in the world via a microphone linked to the computer. Typed messages can also be sent in this way. Educational chat rooms are gradually being developed which would allow learners to experience this facility in a safe environment. Use of unmoderated "chat rooms" can be extremely hazardous and is not appropriate for educational use. A number of chat

rooms are available which are perfectly safe for learners to use as they are closely monitored and restrict access – www.gridclub.com is an example of a popular site for primary pupils with chat facilities. For information which could be discussed with pupils, www.chatdanger.com has examples about the dangers of chat rooms plus guidelines for safe chatting.

14 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. This facility is blocked in schools.

15 Data Protection

Personal information about other users should never be revealed over the Internet. Full details of policy and procedures relating to this topic can be found in the SBC Document: "Code of Practice on the Data Protection Act".

16 Virus Protection

All SBC computers used for access to the Internet are installed with anti-virus software. This software is 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 users should be aware of the issues and the risks. Any user who suspects the presence of a computer virus must alert the appropriate Help Desk immediately!

17 Copyright

Copyright rules also apply to material available over the Internet, and such material will generally be subject to the same level of protection as material in other media. Although there are no specific exceptions from copyright material on the internet, those relating to, for example, fair-dealing for the purposes of non-commercial research or private study may apply.

Many websites carry copyright notices setting out precisely how the material may be used and how to obtain permission. The following information gives basic guidelines – if you are unsure or have specific concerns you should seek further advice:

- Always acknowledge sources.
- Never assume that educational use of material is permitted, without first checking with the author. Be aware that web-based resources may themselves have been published without the appropriate permissions. Therefore, any subsequent use of such material may also be illegal.
- Staff and learners should be aware that work they publish on eg a school website 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 on a school website.

- Using a website live in a lesson is not a breach of copyright, but copying an entire page into, without appropriate permission, 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 without appropriate permission would be.
- Remember that copyright laws vary between countries – the website being used may have been created abroad
- (See Appendix F copyright example from the BBC)

18 School 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.

“If a website includes a pupil’s picture, then this could be downloaded from the web, and edited in an unpleasant or embarrassing way. This new image could be circulated via newsgroups or on another webpage... Parents have concerns that information about their children may be made available worldwide by schools, and that their children can be identified and traced..... A pupil could be traced if their name and picture appear on the school’s website. It would be possible for them to be contacted by someone wishing them harm.” (Click Thinking – Scottish Executive)

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. Website developers should ensure that young peoples’ safety and rights are not compromised i.e. Young peoples’ names should not appear in websites.

Photographs of individual young people should not be posted in websites.

- Photographs of groups of young people may be posted but only with written parental permission for all members of the group.
- Schools should ensure that parents are fully informed of these procedures and the reasoning behind them.
- The SBC Admission Form has a section requiring parents to consent to a Pupil’s photograph being used on any school or council website. See [Appendix A](#).

The current SBC logo should appear (unedited) on all education websites.

19 Mobile Phones, PDAs and Digital Cameras in Schools

Mobile equipment can be used to send and receive text, pictures and video. They therefore have significant potential for abuse. However many parents feel that they wish their child to carry a mobile phone for reasons of personal safety. It is therefore not appropriate to impose an outright ban. The following rules should be followed to minimize the risk of inappropriate or illegal use of these devices on school premises:

- In High Schools, mobile phones must be completely switched off during all teaching experiences - classrooms, sports, assemblies and moving between classrooms. It is not sufficient to switch devices to a “silent” or “vibrating” setting. Use at lunchtime and intervals may be permitted where the rules of safe use are followed.
- In primary schools, mobile phones must be switched off for the entire school day. Emergency contact can be arranged through the school office.
- Many mobile phones are multi function devices and include MP3 players, cameras etc. All such functions must be switched off as described above.
- Inappropriate use of text messaging is not allowed at any time.
- Digital video or still cameras should only be used as part of a planned lesson with teacher supervision. No photographs video or sound recordings can be taken without the express approval of the subject (whether pupils or staff).
- Bluetooth technology should not be used on school premises to transfer images at any time. There is a danger that such images can be picked up by other Bluetooth enabled devices in the vicinity.
- These rules apply to any equipment offering the same functions as mobile phones.
- Breaking any of these rules will be regarded as a breach of school disciplinary policy and appropriate action will be taken according to the school’s behaviour management policy.
- Serious cases of intimidation and bullying with such devices should be referred to the police.

20 Social Networking Websites

There are a number of sites such as Bebo and YouTube that allow individuals to post their own pages with info, pictures and recordings. These sites are highly popular with young people. Access to these sites is blocked on school networks because of the large amount of inappropriate and illegal material contained there. However, pupils can access these from home. There have been some incidents of pupils posting offensive material about fellow pupils and staff on these sites. It is important that schools educate pupils about responsible use of such sites, but neither schools nor the local authority can be expected to monitor or manage access by pupils from home. Posting to any of these sites is password protected and can therefore be traced back to the user. Any incidents of these sites being used for offensive or inappropriate references to other pupils or staff should be

referred directly to the police.

21 Digital Imaging

The SBC School Admission Form has a section relating to parental consent being required for the use of pupils' images in photos or digital videos. This consent is sufficient and covers SBC legal obligations. It should be noted, however, that this is for 'Educational Use' of these images only.

If a school wishes to feature certain pupils very prominently in, for example, a digital video for school use, then additional permission from parents might be recommended. At no point should such materials be used for commercial purposes.

22 Videoconferencing

When using video-conferencing you should apply the same policy as for displaying information about learners on a web site. It is possible, though unlikely, that someone could eavesdrop on your conference and record sound and vision. Learners should never give out any personal information in a conference, including full names, addresses, phone numbers, etc.

23 Advice to learners

Information to learners on Internet safety should include:

- Make sure that you never tell anyone you meet on the Internet personal details such as your home address, phone numbers, photos or bank details
- Make sure that you never tell anyone you meet on the Internet your school's name or phone number.
- Never arrange to meet in person someone you first met online
- Remember that not everything you read online is true – if an offer seems 'too good to be true', it probably is

Advice on safe use of the Internet should be part of ongoing Personal and Social Development (PSD) courses. 'Pupils' Personal Safety' is a new section of the [SBC ICT website](#). The sites listed can be used to raise learners' awareness of safety issues across a range of communications devices and would support teacher / pupil discussion in a PSD or Health and Safety unit.

24 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 referencing it in their School Handbook.

25 Dealing with possible misuse in school

Schools should have a system of immediate sanctions, as part of the Behaviour Management Policy, for dealing with improper use of ICT equipment and its use.

26 Child Protection

Child Protection is a serious issue and any incidents, which cause concern, must be dealt with in line with **SBC 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.

27 This policy – monitoring and responsibility

The effectiveness of this policy will be monitored on a 3 yearly basis by the ICT Manager, E & LL, in conjunction with the department's Schools and Community Services Managers and Communications & Policy Manager. The first review will be September 2010.

28 Version Control

A Policy for Safe Use of Internet Technology	Version Number: 1
Date first approved: 29 January 2008	Approved by: Education Executive

Education & Lifelong Learning
 Council HQ
 Newtown St Boswells
 Melrose
 TD5 7RZ
 Tel: 01835 824000

GLOSSARY

Content filtering software	Software used in schools to block access to websites that may be illegal or unsuitable.
Data protection	A process for secure storage of information held on computers.
Digital Imaging	Computers store information in a digital form which allows accurate repeated reproduction. Sounds and images stored in this way can be easily edited.
File transfer protocol (FTP)	Transfer of computer files across the internet
General Teaching Council for Scotland (GTCS)	An organisation which controls entry to the teaching profession.
Instant Messaging	Instant messaging is a small window where two or more people can chat using text messaging. Usually IM is used for person-to-person chat.
Intellectual Property Rights (IPR)	Rights granted to creators and owners of works that are results of human intellectual creativity.
Internet Newsgroups	Forums for exchanging information and views over the Internet. When you post a message it is copied around the world, using newsgroup servers on the Internet, so other people can read it and reply with their views
Internet Relay Chat (IRC)	Allows internet users to be on line at the same time. They communicate by sending text messages which appear on screen.
Internet Service Provider (ISP)	Organization with a direct connection to the internet allowing other users to connect and providing them with e-mail addresses.
Media Messaging	Sending pictures, videos and sounds electronically
Palmtop	A hand held or pocket computer, like a personal organiser, which can be used as a diary, for note taking or email.
Personal Digital Assistant (PDA)	A hand held or pocket computer, like a personal organiser, which can be used as a diary, for note taking or email.
Video conferencing	Allows people to communicate at a distance with sound and images, either via the Internet or high speed telephone lines, using a camera and microphone attached to a computer.
Video streaming	Allows users to watch films, video or TV on a computer, as they are being broadcast.
Virus protection	Protects computers and networks from software designed to cause damage.
Wireless network	A network where computers can communicate with one another through radio links, without being physically connected.

Index		Page
1	Purpose of the Policy	1
2	Corporate Context	1
3	Accessibility Statement	1
4	Background	1
5	Responsibility	2
6	Supervision in Schools	5
7	Acceptable Use Policy	5
8	Use of the Internet	5
9	E-mail	6
10	Staff Use of Email	7
11	Internet News Group	7
12	The Use of File Transfer Protocol (FTP)	7
13	Use of Internet Relay Chat (IRC)	8
14	Use of Instant Messaging	8
15	Data Protection	8
16	Virus Protection	8
17	Copyright	8
18	School Website Development	9
19	Mobile phones, PDAs and Digital Cameras in Schools	10
20	Social Network Websites	10
21	Digital Imaging	11
22	Videoconferencing	11
23	Advice to learners	11
24	Informing Parents	11
25	Dealing with possible misuse in school	12
26	Child Protection	12
27	This policy – Monitoring and responsibility	12
28	Version Control	12
	Glossary	13
	Index	14
	Authors	15
Appendix A	SBC Guidelines on the use of digital images of learners	17
Appendix B	Exemplar School Policy – a starter document	18
Appendix C	Acceptable Use Agreement – Letter to parents	23
Appendix D	Acceptable Use Agreement – Pupil's form to be signed	25
Appendix E	Net Rules	27
Appendix F	Copyright Information	30
Appendix G	General Teaching Council for Scotland : Excerpts from publications	31
Appendix H	Links to sources of additional information	32
Appendix J	SBC Library and Information Service Acceptable Use Policy	33

Authors	
Liz Marroni	Principal Teacher – ICT
Gladys Purves (Earlston Primary)	ICT Masterclass
Dorothy Coe (St Peter's Primary)	ICT Masterclass
Iain Anderson (Hawick High)	ICT Masterclass
Douglas Angus (Kelso High School)	ICT Masterclass
Revised by	
Helen Cotton	ICT Manager
Consultation	
Child Protection Group	
Henry Thompson	Head of Corporate IT
Leona Bendall	Communications and Policy Manager
Community Services Managers	

Acknowledgements

We would like to acknowledge the support of colleagues in Scottish Borders Council Schools, and also Aberdeen City Council Education ICT Department for their willingness to share their exemplar materials.

Appendices

Appendix A	Use of photos - Excerpts from SBC School Admission Form
Appendix B	Exemplar School Policy (This is only included as a starter document and can be edited, amended and augmented to suit individual schools' circumstances.)
Appendix C	Acceptable Use Agreement – Letter to parents – Primary Pupils (Exemplars) - Letter to parents - Secondary Pupils
Appendix D	Acceptable Use Agreement (Exemplar)
Appendix E	Net Rules Posters
Appendix F	Copyright Information from BBC (Adapted from Aberdeen GfL)
Appendix G	GTC : Excerpts from publications
Appendix H	Links to sources of additional information
Appendix J	SBC Library and Information Service Acceptable Use Policy

Appendix A Use of photos

These excerpts are taken from the SBC School Admissions Form

DATA PROTECTION ACT 1998		
PHOTOGRAPHS AND VIDEOS		
<p>Photographs and videos are taken by the school for a variety of reasons, for example Sports Day, celebrations of achievement, charity events, excursions, etc. We wish to publicise the many activities in which our pupils participate and therefore would like to display photographs throughout the school and in some cases local press may seek permission to use these photographs or take their photographs of pupils. We may also want to use photographs of children on the school's own or Council website.</p>		
	Please tick	
	YES	NO
Do you consent to your child being photographed / videoed for school or press purposes?	<input type="checkbox"/>	<input type="checkbox"/>
If you answered Yes to a photograph being taken, do you further consent that your child's name may be released to the press?	<input type="checkbox"/>	<input type="checkbox"/>
Do you consent to your child's photograph being used on the School or Council website. We undertake that your child will never be named in any School or Council website use.	<input type="checkbox"/>	<input type="checkbox"/>

Also from the SBC School Admissions Form

INTERNET RESPONSIBLE USE AGREEMENT
<p>The School uses Internet resources as part of its curriculum. It is Council Policy not to allow unsupervised access to the Internet.</p> <p style="text-align: center;">Do you consent to your son/daughter having Internet access in a supervised situation?</p> <p style="text-align: center;">Please tick : YES <input type="checkbox"/> NO <input type="checkbox"/></p>

Appendix B Exemplar School Policy

This document is only an exemplar and is not intended to be an all-encompassing Internet Policy document. It may be useful for a school to use as a starting point for discussion, and for editing, according to their own circumstances and with the involvement of their staff.

<Insert School Name> Internet Safety Policy

In <Insert School Name> we recognise that ICT has a clear role to play in meeting aspects of the five national priorities of education in Scotland. The statutory curriculum requires pupils to learn how to locate, retrieve, exchange and present information using ICT. Web-based resources skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill. In the <School name> curriculum, teachers plan to integrate the use of ICT for the benefit of our pupils.

Most technologies present risks as well as benefits. In <Insert School Name> we adopt **the strategies for the safe and responsible use of the Internet in accordance with Scottish Borders Education and Lifelong Learning Department policies.** In line with school policies that protect pupils from other dangers, we endeavour to provide our pupils with as safe an Internet environment as possible and teach them to be aware of and respond responsibly to any risks.

Vigilance and Supervision are our key strategies. In accordance with SBC policy we will take all reasonable steps to ensure that pupils are not placed in an embarrassing or potentially harmful situation. Pupils, teachers, parents / carers, and adult helpers are all asked to play their part in assisting pupils to use the internet responsibly and safely.

Pupils will be discouraged from aimless surfing, not least because it is frequently time consuming and unproductive.

<Insert School Name > Core Principles of Internet Safety

The Internet is becoming as commonplace as the telephone or TV and using it effectively will be essential for success for many pupils in later life. Unmediated Internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and unwelcome situations. Our school's policy helps to ensure responsible use and the safety of pupils.

Our Internet Safety Policy is built on the following five core principles:

Guided educational use

Curriculum use of the Internet will be planned by the teachers, and be focussed on particular tasks within a supervised and managed environment. **Pupils' internet use will be supervised.** We do not believe that pupils' browsing the web in an undirected way is educationally productive.

Risk assessment

Pupils will be taught to use the internet responsibly in accordance with both our School and SBC Policy guidelines. They will be expected to adhere to the Acceptable Use Agreement. Pupils will receive guidance on what to do if they come across inappropriate material.

Responsibility

Internet safety depends on staff, schools, parents/carers and pupils themselves taking responsibility for the use of Internet and other communication devices such as mobile phones. Pupils will be educated to take a responsible approach.

Regulation

The use of our school computer systems requires some straightforward rules and guidance to be in place for everyone's benefit. Misuse, or damage is unacceptable and computer access will be denied if necessary. Chat rooms, other than those intended for educational use, are never allowed to be accessed by anyone in our school. Fair rules, which are clearly understood by pupils through discussion, will be on display beside computers to help them make responsible decisions.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. We base these on limiting access, developing responsibility and on guiding pupils towards educational activities. Staff, parents/carers and the pupils themselves are all expected to show a well informed and vigilant approach.

<Insert School Name> Our Internet Safety Policy

Our Internet Safety Policy is part of the ICT Policy and School Development Plan and relates to other policies including those for Behaviour, for PSD and Citizenship. It also relates to the SBC Policy for Safe Use of Internet Technology.

Why do we use the Internet ?

The purpose of Internet use in <School Name >school is to enhance pupils' educational experience, to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and provides an ever expanding range of global resources for pupils. <School Name >wishes to provide pupils with quality Internet access as part of their learning experience.

The Internet benefits our pupils and teachers, by :-

- providing access to up-to-date world-wide educational resources, including museums and art galleries, plus a wide range of on-line curriculum activities.
- providing staff professional development through access to national developments, educational materials and good curriculum practice;

How will Internet use enhance learning?

- The school Internet access is designed for pupil use and includes filtering
- Pupils will be taught what Internet use is acceptable and what is not and given clear tasks for Internet use.
- Internet access will be planned to enrich and extend learning activities. .

- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of finding relevant information, retrieval and evaluation, together with some understanding of the correct usage of published material.
- For pupils, effective internet use generally involves teachers choosing a topic with care, selecting the search engine, and then discussing with pupils sensible search words, or selecting specific websites, which would be tested beforehand. Pupils will be encouraged where practical to use the Internet in response to a task - e.g. a question arising from investigative work in class.

How will pupils learn to evaluate Internet content?

According to their age pupils, will come to learn and appreciate :-

- that information gained from websites should be used selectively
- that thought should be given to its relevance to the task.
- respect for copyright and intellectual property rights is important,
- that there are correct ways to use published material
- that if staff or pupils discover unsuitable sites, the URL (address) and content should be reported to the teacher, senior member of staff with responsibility for ICT, and the Network Administrator

{ Possible additional statements which schools may wish to incorporate at this point. The following statements will require adaptation according to the pupils' age:

- *Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.*
- *Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.*
- *Guidance should be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.)*

How will pupils use E-mail?

All our pupils are provided with a filtered school email address. The extent to which this will be used will depend on the pupil's age, the curriculum requirements for their stage, and the technical considerations. Our school email is private and is subject to monitoring.

- Pupils will be taught to use this responsibly and safely.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive 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.
- A Whole-class email address may be used by younger pupils.
- Excessive social e-mail use can interfere with learning and may be restricted.

Our school website

This is intended to provide information to parent / carers and others and show selected information about our school and its activities. We hope that our pupils will be inspired to publish work of a high standard. Publication of information will however, be considered from a security viewpoint.

- No recognisable close-up photos of pupils will be placed on our website, nor will any pupil be identified by name.
- Small photographs of groups of pupils, that do not show faces at all, or “over the shoulder” photos may be used to convey the educational value of the activity.
- Staff or pupils’ home information will not be published.
- Parents/carers will be asked for the usual permission on the School Admission Form for consent regarding photos/videos taken for in-school use according to SBC Guidelines

<Insert School Name> follows the SBC Internet Safety policy with regard to:-

Chatrooms

The use of unmoderated chat rooms is not permitted in this school. We may use Grid Club, www.gridclub.com to provide safe and interesting conferencing environments for our pupils aged 7-11.

Outside school, we recognise that pupils may use a variety of chat facilities and may not be fully aware of the potential dangers. Pupils will have opportunities to discuss safe use of chat facilities in their PSD lessons.

Mobile phones

- (For high schools) All mobile phones must be completely switched off during all teaching experiences - classrooms, sports, assemblies and moving between classrooms. It is not sufficient to switch devices to a “silent” or “vibrating” setting. Use at lunchtime and intervals may be permitted where the rules of safe use are followed.
- (For primary schools) All mobile phones must be switched off for the entire school day. Emergency contact can be arranged through the school office.
- Inappropriate use of text messaging is not allowed at any time.
- Use of digital video or still cameras should only be used as part of a planned lesson with teacher supervision. No photographs video or sound recordings should be taken without the express approval of the subject (whether pupils or staff).
- The use of Bluetooth technology is not allowed on school premises.
- These rules apply to any equipment offering the same functions as mobile phones.
- Breaking any of these rules will be regarded as a breach of school disciplinary policy and appropriate action will be taken according to the school’s behaviour management policy.
- Serious cases of intimidation and bullying with such devices will be referred to the police.

Internet Access

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 are informed through the SBC School Admissions Form that pupils will be provided with supervised Internet access.

All school users will be asked to complete an Acceptable Use Form (from p4 onwards)

<Insert School Name> school will take all reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SBC can accept liability for the material accessed, or any consequences of Internet access.

- All internet access will be supervised
- Rules for Internet access will be posted in all rooms where computers are used. (A copy can be made available to parents)
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will be given
- A session on responsible Internet use will be included in the PSD programme covering both school and home use.

Staff

It is important that our teachers and additional assistants are confident to use the Internet in their work.

- Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies.
- All staff including teachers, supply staff, classroom assistants and support staff, will be able to access SBC policies.
- Staff will be made aware of sources of further information on Internet and mobile communications safety
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user.

Security of SBC Networked systems

This responsibility falls within the remit of SBC who maintain and review the security and functionality of the school networked systems. This includes:-

- Virus protection which is installed and updated regularly.
- Maintaining the provision of filtered and audited internet access.
- Installation of hardware and software on the school networks.

The School Policy on Internet Safety will be reviewed as part of the School Improvement Plan, and endeavour to keep in line with technological and networked developments within the SBC and the school.

This document is an exemplar. It may be useful for a school to use as a starting point for discussion, and for editing, according to their own circumstances and with the involvement of their staff.

Appendix C <Insert School Name> - Primary

Dear Parent / Guardian

Responsible use of the Internet. Letter to parents (Exemplar)

At SBC School we want to give our pupils as rich a variety of learning opportunities as possible and allow them to access many educational websites that are available on the Internet. The Internet provides a great wealth of information that can enrich our class work and the ability to use the Internet efficiently is a skill that will be of value throughout a child's life.

In response to concerns about pupils having access to undesirable materials, steps have been taken to diminish the risks. These include staff identifying particular sites or titles for pupils to visit rather than simply allowing them to "surf" the net. All internet use will be supervised. Our school internet service provider also operates a filtering system which restricts access to inappropriate materials.

While the school is making efforts to ensure suitable safeguards are in place to protect pupils, we feel that the pupils themselves must also play their part. For this reason we have drawn up a list of Net Rules for Responsible Internet Use which we ask pupils to agree to, and abide by.

These rules are on display, and have been discussed with pupils. The reasons for their introduction have also been explained. It has been pointed out to the children that anyone deliberately breaking the rules will have their personal access to the internet within school either denied, or at least severely restricted. I have attached a copy of these 'Net Rules' for your information and you may wish to discuss them again with your child.

Once you have read the attached letter and attached rules, we ask that you and your child sign the attached permission / agreement form and return it to school. If your child is old enough, he/she should sign the pupil section. (*We suggest that children from primary 4 upwards will be old enough to understand the rules but individual children will vary.*) Parents and pupils will only be required to sign the agreement once while the pupil is at our school. Parents can also withdraw their permission for internet use at any time

If there are any aspects of internet use you wish to discuss (either before you sign the form, or at any time in the future) please feel free to contact the school.

Yours sincerely
Headteacher

<Insert Name of School> will follow the SBC policy on “Safe Use of Internet Technology” to protect students from unsuitable material. I understand that they will make every reasonable effort to restrict access to all controversial material on the Internet, but I will not hold them responsible for materials my son or daughter acquires or sees as a result of the use of the Internet at school.

Pupil Name:

Class:

Permission for Internet Access

Parent / Guardian’s permission

I give permission for access to the internet on the terms set out in the above letter.

Signed _____

Print name _____

Date _____

Pupil’s agreement (P4 upwards)

I agree to follow the Rules for Responsible Internet use.

Signed _____

Print name _____

Class _____

Appendix D



<Insert Name of School> - Secondary

**Agreement for Computer and Internet Use (Exemplar)
PARENT/GUARDIAN**

As the parent or guardian of

I have read the rules for Acceptable Computer and Internet Use and understand that these rules apply when my child is using school computers and the Internet. I have gone through the rules with my child and explained their importance and the consequences of breaking the rules. I understand that computers and Internet access at <Insert Name of School> are provided for educational purposes only.

<Insert Name of School> will follow the SBC policy on “Safe Use of Internet Technology” to protect students from unsuitable material. I understand that they will make every reasonable effort to restrict access to all controversial material on the Internet, but I will not hold them responsible for materials my son or daughter acquires or sees as a result of the use of the Internet at school.

I give my permission to <Insert Name of School> to allow the student named above to use the computers and Internet in the school. (This can be changed at any time, just contact the Head Teacher.)

Parent's signature _____ **Date** _____

This school may produce web pages, ICT presentations, educational or interest articles for magazines or similar. No child’s work or photograph will ever be used without his/her permission but we also need permission from parents and guardians to be able to publish the child’s work. Please rest assured that the child’s safety will always be of paramount importance and no personal information will be made public. Please sign this copyright release if you are happy for your child’s work to be shared in this way. (This can be changed at any time, just contact the Head Teacher.)

I consent for the school to publish my child’s work or photograph on the Internet or elsewhere, subject to strict confidentiality of personal information.

Parent's signature _____ **Date** _____

STUDENT

I have read the rules for Acceptable Computer and Internet Use and know the importance of these rules. I know that if I break these rules, I might lose the right to use the school’s computer facilities and / or face further disciplinary action.

Student's signature: _____ **Date** _____

Acceptable Use Agreement (Exemplar)

**<Insert Name of School> Acceptable Computer & Internet Use Policy (AUP)**

All computer and Internet use is supervised. When students are allowed to use computers or the Internet, they will be expected to follow these rules:

While using computers or the Internet at SBC School

1. I will only use the computer for educational activities.
2. I will not use bad language in any messages I send.
3. I will not try to visit sites, which might have offensive material.
4. I will inform staff if I find any inappropriate material on a computer I am using.
5. I will not reveal the personal address, phone number or password of others, or myself nor use another's password.
6. I will not use any computer in such a way that would disrupt the computer use of others.
7. I will not attempt to access files belonging to others.
8. I will not interfere with any computer security measures the school may have in place.
9. I will respect copyright and not use anything I download without the approval of a member of staff.

Users should be aware that monitoring and random checks are made on all computer use and e-mail messages sent and received.

All rules relating to computer use apply to computer networks and stand-alone computers in the school.

These rules also apply to all information sent electronically within the school, including text messages or pictures sent by mobile phones.

Appendix E Net Rules – for very young children. (Adapted from Kent Grid for Learning)

Think then Click

These rules help us to stay safe on the internet



We only use the internet when an adult is with us.



We can click on the buttons or links when we know what they do.



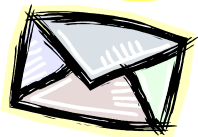
We can go to our favourite websites with an adult.



We always ask if we get lost or are not sure what to do.



We tell an adult if something odd happens.



We can write polite and friendly emails to people that we know.

Net Rules –Primary,

Our Internet Rules

The Internet can be a great place for finding lots of useful and interesting information and for getting in touch with people all over the world. Most people who use the Internet are honest, but to be extra safe, you should always follow these rules.

Log on with your own username and password, or one the teacher has given you.

Make sure that you never give anyone's photograph, address or telephone number over the Internet, including your own.

Make sure that you never give your school's name unless you have permission from your teacher.

Never agree to meet anyone who contacts you on the Internet. Always tell your teacher if someone asks you to do this.

Always tell your teacher if you see anything which makes you feel uncomfortable. Switch off the monitor.

Always tell your teacher if someone sends you a nasty message. Remember it is not your fault if you get a message like this.

Net Rules for use with older students and adults

Net Rules & Responsibilities

- Log on with your own user name and password. Never give your password to anyone.
- Make sure that you never give anyone's photograph, address or telephone number over the Internet.
- Inform the network administrator immediately if any abusive, threatening or offensive e-mails are received.
- Inform the network administrator immediately if any e-mail or attachment generates a virus warning.
- Respect copyright rules for any material available over the Internet.
- The following activities are strictly prohibited:
 - Use of Internet facilities to harass, offend or bully any other person;
 - Use of Internet facilities for any inappropriate or illegal purpose
 - Use of Internet facilities for transmission or reception of threatening or obscene material;
 - Use of Internet facilities for transmission or reception of material from any criminal organisation;
 - Use of Internet facilities for the transmission or reception of viruses or unlicensed software;
 - Use of Internet facilities for any personal commercial purpose or profit.

Appendix F Copyright Information

(Adapted from Aberdeen City Council Curriculum Resources and Information Service)

As outlined in Section 17 material on the Internet is also subject to copyright legislation. Unless there is a specific message on a website allowing you to download freely, you should assume that the material is copyright. Most copyright holders won't mind if you download an article or picture to use with children but will object if you make multiple copies of their materials or use them on something which is available beyond the school such as training materials used in several schools or a web site. If in doubt, contact the web site. Distributing downloaded material electronically is no more acceptable (or legal) than photocopying and distributing printed copyright material.

The BBC provide clear guidelines to schools on the use of material from their website. The guidelines are typical of the kind of use allowed by educational sites.

They can be viewed at www.bbc.co.uk/schools/copyright

A simple example:

Pupils could copy and paste a graphic from the internet into, for example a greetings card (made with their DTP application). The source of the picture should be acknowledged. These 'Greetings' cards cannot subsequently be sold to parents or the general public as part of a commercial or enterprise activity as this would infringe copyright rules. Pupils should not be encouraged to copy/paste internet text directly into their own documents without acknowledging their sources. . They should be encouraged to be selective about the information and re-write using their own sentences.

Appendix G General Teaching Council for Scotland - Excerpts from publications

GTCS - Professionalism in Practice

Inappropriate Material, the Internet and E-mail

It is essential that a teacher avoids situations both in and outwith the classroom which could bring him/her into conflict with the Criminal Law or have an actual or perceived impact upon his/her standing as a teacher. Notwithstanding an individual's right to a private life, a teacher should, for example:

- not have in his/her possession at any time illegal materials/images in electronic or other format;
- not have in his/her possession inappropriate materials/images on school premises;
- not download or access illegal images at anytime or in any place;
- not access inappropriate sites or download inappropriate materials on school premises;
- ensure that he/she is fully aware of his/her employer's ICT guidelines and adhere to them;
- all communications with pupils/students must be justified in terms of learning and teaching. In any event this should be carried out in a professional manner using an official school email address and in strict compliance with employer ICT
- policies;
- exercise extreme caution in connection with contact/web cam sites (for example chat rooms, message boards and newsgroups) and not engage in communication with individuals under 18 or with whom he/she is in a position of trust.

Professional Integrity

All staff/pupil relationships must be professional, appropriate and justifiable. Teachers should adhere to common sense and avoid inappropriate situations. Teachers are entitled to a private life; however they must be conscious that they are role models for their pupils and students and that young people, in particular, may be strongly influenced by the conduct of teachers whether within or outwith the classroom. Teachers should avoid inappropriate relationships with pupils or students. Photographing/making videos of pupils/students must comply with the guidelines laid down by employers.

Appendix H Links to sources of additional information

General – Excellent starting Point

<http://www.itscotland.org.uk/ictineducation/ictadvice/internetsafety.asp>

This site has links to all the major Educational Internet Safety Organisations

For Pupil / Teacher use

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

www.educationict.org.uk/guidelines.htm (Scroll down to the Pupil Personal Safety Section)

For Parents

Pamphlets for parents: <http://www.kidsmart.org.uk/parents/usingks.aspx>

Information

http://www.besafeonline.org/English/safer_use_of_services_on_the_internet.htm

Instant Messaging

http://www.besafeonline.org/English/instant_messaging.htm

Mobile Phones

Mobile Phone Safety Project - a [printable pamphlet](#) with mini-case studies for discussion with older learners. Teacher's guidance notes on how they can be used in class.

Gridclub Cybercafe – good mobile phone advice, presented as a series of [interactive activities for primary learners](#)

Citizenship activity about [Mobile Phone Crime](#) for upper primary and secondary learners

Copyright and Intellectual Property

Copyright Licensing Authority

[CLA http://www.cla.co.uk/support/schools/schools-support-licence-eng.pdf](http://www.cla.co.uk/support/schools/schools-support-licence-eng.pdf)

Website Development

[‘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.

Appendix J SBC Library and Information Service Acceptable Use Policy

1. Introduction

Scottish Borders Council Library and Information Service provides free access to Computers and the Internet in keeping with its objective to meet and support the cultural, educational and recreational needs and aspirations of people living and working in the Scottish Borders area.

2. The Internet & your responsibility

Whilst the Internet contains a wealth of valuable and interesting information some of this information may be inaccurate, out of date, controversial, offensive and/or illegal. The Library service accepts no responsibility for the quality, accuracy or availability of information accessed through the Internet. The Library Service will not be liable for any direct or indirect, incidental, or consequential damages (including lost data or profits) sustained or incurred in connection with the use, operation, or inability to use the computer resources.

3. Conditions of Access

Membership

Access to computers in the Scottish Borders Library Service is available to all. All users must accept the Scottish Borders Council Library and Information Service Acceptable Use Policy before they can use the computers. A brief version is displayed on the screen and the full version is available in the library.

Children and young people

Under 16 year olds may use this service with the written consent of a parent or guardian who must agree that they have read and accept the Acceptable Use Policy.

Cost

While the use of Internet computers is free of charge, a charge will be made for printing and all items printed will be charged for at the advertised rates.

Booking a computer session

- Sessions may be booked up to two weeks in advance by telephone or in person.
- Users can have 3 active bookings at any one time.
- A session may be extended if someone else does not need the computer.
- No more than two people may use a computer at any one time, at the discretion of library staff.

4. Your session in progress

Library staff can provide limited help to users in the proper use of the computers, and provide help in identifying and accessing useful sites. Library staff cannot provide extended tuition in the use of computers. They can provide information about local computer courses, self-help manuals, and other computing books held in library stock.

Scottish Borders Council Library Service may monitor logs showing access to Internet sites, and any public access of illegal, offensive or controversial material may be the

subject of further action. Monitoring of computer usage can be performed electronically and manually.

5. Security

Filtering

Our policy on access is informed by the freedom of information principles, applying to the provision of all library material. We believe that it is in the freedom of information interests of adult service users to manage our web provision without the use of filtering software. Filtering is however applied to all junior access to services. Current filtering technology cannot block all offensive sites and sometimes may inadvertently block legitimate sites that we would wish to provide access to. Because of the limitations of filtering technology the Library Service cannot guarantee against users accidentally accessing information and images they might find offensive or disturbing.

Virus-checking software will run on all computers.

Computers will automatically reboot and reset when a user logs out so all information or files which a users wants to keep must be saved to floppy disk or CD-ROM before the end of their session. Users may install their own software only if they have a licence for it and it does not require the PC to be rebooted. Users may be able to connect their own equipment to library computers but must ask a member of library staff for assistance.

Information downloaded from the Internet must be downloaded within copyright and licence restrictions to a floppy disk or CD-ROM.

6. Parental responsibility and Child Safety

PCs are filtered when used by children **however Filtering software cannot block all offensive sites** and is designed to limit not completely block access to unsuitable sites. Library staff cannot supervise the use of this service and the Library Service cannot take responsibility for any material accessed which a parent or guardian may consider unsuitable. Parents and guardians who are concerned about the types of materials available on the Internet should work with their children and help them to select resources consistent with their family's values and boundaries. Some recommended sites are listed under our children's pages on our web site. Please notify staff if you /your child does access inappropriate material by mistake and we will investigate.

7. Prohibited Uses

Scottish Borders Council Library and Information service do not prohibit specific online activities except those which are considered to be illegal, offensive, obscene, abusive or troublesome to other computer users. Users should be aware that risks are attached to some online activities

- Broadcasting personal or private details over the network may lead to the receiving of unwanted mail or unwanted attention
- Online financial transactions are an increasingly common use of the Internet and designed to be conducted safely over secure connections. However Scottish Borders Council Library and Information Service cannot be held responsible for any losses resulting from sending confidential financial information via the Internet

- Some online activities (e.g. game playing) can seriously impact on the ability of the network to deliver other services. Scottish Borders Council Library and Information Service reserve the right to restrict access to such services

Users must not interfere with equipment

Computers may not be used to create, access, copy, store, transmit or publish material that may be inaccurate, defamatory, illegal, or potentially objectionable to some people

Users must not make any attempt to gain unauthorised access to any restricted files or networks, or to damage or modify computer equipment. This includes the transmission or reception of viruses.

The Library provides access to the Internet and its information and services for the use of its library members and casual users.

8. Responsible use of the Internet:

- Library users must respect the privacy of other users, and refrain from attempting to view or read material being used by others.
- Users are required to respect copyright laws and licensing agreements. Please ask library staff if you are unsure.
- Users who incur charges for printing or other authorised fees are required to pay promptly
- Users are required to end their session and leave the PC if asked to do so by authorised Library staff.

9. Penalties for misuse

A Library staff member will direct computer users to remove inappropriate images or text from the screen if, in the staff member's judgement, the image or text is likely to cause offence to other library users

Library staff are authorised to terminate any user's access session if they believe that the user has failed to comply with the Acceptable Use Policy. Computer privileges will be suspended, at a minimum, for the rest of the day and staff will file an incident report.

All complaints will be investigated and a written warning followed by a formal notice of suspension may be issued. If illegal use is identified suspension will be immediate pending police investigation and action. As well as the loss of computer privileges other disciplinary options may be applied, including criminal prosecution. In the case of a junior computer user who violates this Acceptable Use Policy, the parent or guardian who signed the Computer Use Registration Form will be notified.

All libraries display our Acceptable Use Policy which adult users must accept before they can gain access to the PC.

This policy will be reviewed regularly to ensure that it remains up to date and relevant.

Revised 16th January 2006

SCOTTISH BORDERS COUNCIL LIBRARY & INFORMATION SERVICES

UNACCEPTABLE USE OF LIBRARY PCs – GUIDELINES FOR STAFF

Access to the Internet is available in all SBC public libraries, and because the Internet is unlicensed and uncontrolled, there will be occasions when members of the public will access material which is unacceptable viewing in a public library and which may prove to be illegal.

The following guidelines are provided to give staff a course of action to follow in the event of unacceptable use occurring in the library.

Staff have a responsibility to ensure that they are aware of what constitutes unacceptable use, as laid down in the SBCLIS Acceptable Use policy, and to ensure that everyone using the public access computers is made aware that an Acceptable Use policy is in operation. A copy of the Acceptable Use Policy is available on the Library & Information Services website on

<http://www.scotborders.gov.uk/libraries/content/acceptableuse.html>

Unacceptable use in a public library can be defined as anything that causes offence or upset to other library users or members of staff. What is deemed to be unacceptable may vary with individual tastes and preferences.

Examples would be

- adult content sites
- sex sites which provide graphic images or descriptions of sexual nature
- racism and hate sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.
- tasteless sites with content that is gratuitously offensive or shocking
- violent sites that feature or promote violence or bodily harm.

Accessing these sites would be deemed unacceptable but they are not necessarily illegal.

Some computer use would be both unacceptable and illegal e.g.

- criminal or unethical activity sites e.g. drug dealing
- terrorism or bomb-making
- incitement to riot or violence
- hacking and computer piracy sites
- child pornography

What to do...

Unacceptable Use

If staff have witnessed a breach of the acceptable use policy, staff should use the message facility on the booking system or terminate the computer sessions of user concerned, if it is appropriate to do so.

If staff suspect, or receive a report of, unacceptable use, they should note the date, time the incident took place, p.c. user details and p.c. number and report the details SBCLIS IT staff requesting PC logs be checked

Once IT logs have been checked at Library HQ, SBCLIS IT staff will report the results of the check to the library. Library staff will be advised whether or not to send out a letter to the library user as noted in the Acceptable Use Policy.

Illegal Use

If the check reveals that illegal use is suspected, SBCLIS IT staff will forward details to Lothian & Borders Police for further checking, advise the library what is happening, and advise the LIS Manager, who will keep the Cultural Services Manager informed.

Illegal Use involving children

In the event that unacceptable use proves to be illegal and raises issues of Child protection, the E&LL Child Protection Policy should be followed. SBCLIS IT staff will contact the Child Protection Unit directly and take action as directed by the CPU team. SBCLIS staff will also inform the LIS Manager who will advise the Cultural Services Manager.

If SBCLIS IT staff or a senior manager are not available (weekends or late nights), staff should follow the Child Protection policy, and contact the Child Protection Unit directly for advice. Illegal use should be reported as soon as possible to SBCLIS IT staff, so that checks can be carried out.

NB

Any incidence that raises issues of Child Protection should be reported as soon as possible to SBCLIS Child Protection Co-ordinator, SBCLIS IT staff or directly to the Child Protection Unit.

If the police decide to press charges, SBCLIS IT staff will advise libraries what action they should take. SBCLIS IT staff will liaise with the police and police computer forensic team and with front line staff to ensure that appropriate action is taken to allow the police to gather and preserve evidence from the library computers.

SBCLIS IT staff will also advise the LIS Manager and the CP Co-ordinator that the police are pressing charges, so that senior management and CP staff can be advised accordingly.

Other points to note....

- Read the Acceptable Use Policy & know what is in it
- Be aware of unusual behaviour e.g. flicking to another screen if staff approach
- If unacceptable use turns out to be illegal use, and the case comes to court, it is inevitable that there will be press/ media interest. Staff should not give statements, interviews or information to the press, but should direct all enquiries to SBC Public Relations, who will handle responses on behalf of the Council.

Staff Guidelines /MM&SM/ 1.2.06