1 Cyber Safety Policy

1.1 Introduction

Due to the rapid speed of technological innovation, Internet technology and the schools use of technological resources that will continue to develop and change with time. It is our intention to review and up-date our Internet Safety Policy as appropriate and where necessary.

This policy is part of a series of inter related policies for the safety and wellbeing of students, parents, volunteers, visitors and any other person who comes onto the school site.
This policy should be read in conjunction with the following other site policies:

- Acceptable use of Technology and the Internet
- Mobile Phone Policy
- Anti-Bullying Policy
- Behaviour Management policy

At English Language School we believe:

All people in our community have the right, to teach and learn in a supportive, caring and safe environment, without fear of being bullied.

We believe that every individual in school has a duty to report an incident of bullying whether it happens to themselves or to another person.

Learners experience an expansive array of learning opportunities to meet their academic and social needs.

Learners will participate in an educational program constructed and evaluated on the stable foundation of a dynamic curriculum and administrative policies.

Learners will experience a positive, safe environment in which all partners and resources are respected and valued.

At English Language School, pupils are taught to:

Understand how to use these technologies safely and know about the risks and

consequences of misusing them.

Know what to do if they or someone they know are being cyber bullied.

Report any problems with cyber bullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

English language school has:

An Acceptable Use Policy: that includes clear statements about use of Cyber-communications.

A Cyber Safety and Anti-Bullying Policy: that includes clear statements about Cyber- Safety and how to keep safe with technology.

Information for parents on: E-communication standards and practices in schools,

- What to do if problems arise.
- What is being taught in the curriculum.

Support for parents and pupils: if cyber bullying occurs by: assessing the harm caused, identifying those involved, taking steps to repair harm and to prevent recurrence.

1.2 Statement of Position

The measures to ensure the cyber-safety of English Language School outlined in this policy document are based on our core values.

The school's computer network, Internet access facilities, computers and other school ICT equipment / devices bring great benefits to the teaching and learning programmes at English Language School and to the effective operation of the school.

Our school has rigorous cyber-safety practice and education programs in place, which include Appropriate Use agreements for all school staff and students.

We also provide up to date information to enable families to maintain their children's safety at home. The overall goal of the school is to create and maintain a cyber-safe culture which is in keeping with the values of the school, and legislative and professional obligations.

All students will be issued with a use agreement and internet safety rule agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment / devices.

This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety and bullying breaches which undermine the safety of the school environment.

Important terms used in this document:

'ICT', the abbreviation **'ICT'** in this document refers to the term „Information and Communication Technologies.

'Cyber-safety,' refers to the safe use of the Internet and ICT equipment / devices, including mobile phones.

'School ICT,' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined below.

'ICT equipment/devices,' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, video tape, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.

'Objectionable' / 'Inappropriate material', in this agreement means material that deals with matters such as sex, cruelty, discrimination or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment. This is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993.

'Cyber bullying', is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as email, chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another person.

'E-crime', occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

1.3 Cyber Safety

Cyber Safety encompasses technologies such as the Internet, and electronic communication devices including mobile phones and other wireless technology. With increasing sophisticated and affordable communication technologies, there is a real need for children and young people be thoroughly informed of both the benefits and risks of using these new technologies and provides safeguards and awareness for users to enable them to control their online experiences and the appropriate use of all technologies

The Technologies included in Cyber-Safety:

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. The Current and emerging technologies used in school and more importantly in many cases, used outside of school by children include:

- The Internet
- email
- Instant messaging (msn, aol) which often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (myspace, piczo, bebo, hi5, facebook, twitter)
- Video broadcasting sites (youtube)
- Chat Rooms (teenchat, habbohotel)
- Gaming Sites (neopets, miniclip, runescape, clubpenguin)
- Music download sites (apple, napster, kazzaa, livewire)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are „internet ready".
- Smart phones now come with e-mail, web functionality and cut down "Office" applications.
- X-Box and Play Station (these also have the capacity of internet connection)
- Other applications or technologies still to be released.

Cyber-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of cyber-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- National Education Network standards and specifications

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the Internet may give children access to undesirable information or images.

Children are regularly reminded that should they encounter inappropriate material on line they must immediately:

Turn off the screen.

Report immediately to the teacher or supervising adult who will record the URL and other details.
Refrain from describing or encouraging others from accessing the site either directly or through a search engine.

Should a child or teacher encounter unsuitable material through using the DECS Connect service, this will be reported to DECS CONECT helpdesk number as a matter of urgency by the site administrator.

1.4 Steps Taken to Protect Children

Use of a Filtered Service:

Access to the Internet is provided through a filtered service. All access is provided through the DECS service which is designed to filter out unsuitable material.

Supervision:

No filtering service is 100% effective; therefore all children's use of the Internet is to be supervised by an adult.

Planned Activities:

Use of the Internet is a planned activity. Aimless surfing is not allowed. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

Websites:

Websites are previewed by teachers and revisited to ensure that they are suitable for Children's curriculum needs and ability levels.
Search engines are used selectively. Teachers will choose the search engine and topic and discuss sensible search words which have been tried out beforehand.

Email:

Student use of email is supervised by an adult. While all efforts are made to ensure that messages sent and received are appropriate, it relies on the honesty and integrity of the students themselves to adhere to the ICT Code of Conduct (see Acceptable Use of Technology and The Internet Policy).

Internet Safety Rules:

Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

English language school Website:

On our School Website:

- Children are only referred to by their first names.
- Any images of children will not be labelled with their name.

- No close-up pictures of children will be made available on line.
- Children and teachers will not reveal their personal details, home addresses or telephone numbers on the website.

NB. Pupils' photographs may be published subject to the strict safeguards listed above. If you have any concerns or objections please contact the school to discuss them.

1.5 Safety Points for Students to Consider

- Only use your own login username and password to access computers, Internet or any other technological equipment.
- DO NOT look at, change or delete other people‟s work / files.
- DO NOT change or delete any of the settings on school property.
- Ask permission before entering any website, unless a teacher has already approved that site.
- Only send an email which a teacher has approved and has seen. Make sure that the messages are polite and sensible.
- When sending email DO NOT give your name, address or phone number or arrange to meet anyone.
- DO NOT give the name, address or phone number of anyone else.
- DO NOT enter Internet Chat Rooms while using school computers.
- If you see anything you are unhappy with or you receive messages you do not like: Turn off the screen and tell a teacher immediately. (use the "Hector Safety Button" if available).

1.6 Cyber Bullying

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example: Sending threatening or abusive text messages or e-mails, personally or anonymously

Making insulting comments about someone on a website, social networking site (eg: MySpace) or online diary (blog)

Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail (such as „Happy Slapping" videos)

It should be noted that the use of ICT to bully could be against the law. Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the Harassment Act 1997 or the Telecommunications Act 1984 for example.

It should be noted that the use of the web, text messages, e-mail, video or audio to bully another pupil or member of staff will not be tolerated.

There are many types of cyber-bullying. Although there may be some of which we are unaware, here are some of the more common:

Text messages – that are threatening or cause discomfort – also included here is "Bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology.

Picture/video-clips - via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.

Mobile phone calls – silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.

Emails – threatening or bullying emails, often sent using a pseudonym or somebody else's name.

Chat room bullying – menacing or upsetting responses to persons (children, young people or adults), when they are in web-based chat room.

Instant messaging (IM) – unpleasant messages sent while children conduct real time conversations online using MSM (Microsoft Messenger) or Yahoo Chat; although there are others.

Bullying via websites – use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo (which works by signing on in one's school, therefore making it easy to find a victim) and Myspace – although there are others.

1.7 Information for Parents

At English Language School, we take this form of bullying as seriously as all other types of bullying

and, therefore, will deal with each situation individually.

An episode of Cyber Bullying may result in a simple verbal warning. It might result in a parental discussion.
Clearly, more serious cases will result in further sanctions.

Technology allows the user to bully anonymously or from an unknown location, 24 hours a day, 7 days a week.

Cyber-bullying leaves no physical scars so it is, perhaps, less evident to a parent or teacher, but it is highly intrusive and the hurt it causes can be very severe.

Young people are particularly adept at adapting to new technology, an area that can seem a closed world to adults. For example, the numerous acronyms used by young people in chat rooms and in text messages (POS – „Parents Over Shoulder", TUL – „Tell You Later"; there are many others and they change frequently) making it difficult for adults to recognise potential threats.
Incidents of known or suspected cases can be reported to the principal of the school by email kaneezalicity@yahoo.com

1.7.1 Points for Parents to Consider at Home

It is important to promote phone and Internet Safety in the home, and to monitor Internet use.

Tips to Promote Phone and Internet Safety at Home:

- Know the „SMART" tips.
- Discuss the fact that there are websites which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information on the Internet.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school.
- Mobile Phones; be aware of the safety issues regarding mobile phones. Increasingly these now have Internet access.
- Encourage children to talk about how they use mobile phones.
- Remind children not to give mobile numbers to strangers and people they do know very well.
- Talk about responsible use of text messaging.

1.7.2 Monitor Internet Use

- Keep the computer in a communal area of the home.
- Ask children how the computer works.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing.
- Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner.
- Check internet history log. This will tell you what websites your child is frequenting.

1.8 Information for Students

If you are being bullied:

Remember, bullying is never your fault. It can be stopped and it can usually be traced.

Don't ignore the bullying. Tell someone you trust, such as a teacher or parent or call an advice line.

Try to keep calm; if you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.

1.8.1 Internet

Don't give out your personal details online – if you're in a chat room, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.

Keep and save any bullying emails, text messages or images. Then you can show them to a parent, teacher or police as evidence.

If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

There is plenty of online advice about how to react to cyber bullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips.

1.8.2 Emails

Never reply to unpleasant or unwanted emails (flames‘) – the sender wants a response, so don‘t give them that satisfaction.

Keep the emails as evidence and tell an adult about them.

Ask an adult to contact the sender‘s Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com

Never reply to someone you don‘t know, even if there‘s an option to „unsubscribe‘. Replying simply confirms your email address as a real one.

1.8.3 Text & Video Messaging

You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you‘ve changed your phone number.

If the bullying persists, you can change your phone number. Ask your mobile service provider about this.

Don’t reply to abusive or worrying test or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.

Don’t delete messages from cyber bullies. You don’t have to read them, but you should keep them as evidence.

Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you’ve received.

1.8.4 Phone Calls

If you get an abusive or silent phone call, don‘t hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off.

Once they realise they can’t get you rattled, callers usually get bored and stop bothering you.

Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what’s going on.

Don’t give out personal details such as your phone number to just anyone. Never leave your phone lying around.

When you answer your phone, just say „hello‘, don’t give your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they’ve got the right number or not. You can use your voicemail to vet your calls. A lot of mobiles display the caller’s number. See if you recognise it. If you don’t, let it divert to voicemail instead of answering.

Don’t leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again. Almost all calls nowadays can be traced. If the problem continues, think about changing your phone number.

If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording along too.

If you get an abusive or silent phone call, don’t hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can’t get you rattled, callers usually get bored and stop bothering you.

Text harassment is a crime. Don’t delete messages from cyber bullies. You don’t have to read them, but you should keep them as evidence. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you have received.

If the calls are simply annoying, tell a teacher, parent or carer. Almost all calls nowadays can be traced.

1.8.5 Three Steps to Stay out of Harm’s Way

1. Respect other people – online and off. Don’t spread rumours about people or share their secrets, including their phone numbers and passwords.
2. If someone insults you online or by phone, stay calm - and ignore them.
3. Do as you would be done by‘. Think how you would feel if you were bullied. You’re responsible for your own behaviour – make sure you don’t distress other people or cause them to be bullied by someone else.

1.9 Guidance for Staff

“Bullying can be done verbally, in writing or images, ***including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites.*** *It can be done physically, financially (including damage to property) or through social isolation”.*

Verbal bullying;
This is the most common form of bullying.
Making insulting comments about someone on a website, social networking site (eg: MySpace)

or online diary (blog)

Visual bullying:

Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail (such as „Happy Slapping videos)

It should be noted that the use of ICT to bully could be against the law. Procedures for cyber-bullying are as follows. It should be noted that the use of the web, text messages, e- mail, video or audio to bully another pupil or member of staff will not be tolerated.

Bullying Incident Directed at a Child; occurs using email or mobile phone technology either inside or outside of school time.

1. Advise the child not to respond to the message
2. Secure and preserve any evidence
3. Refer to relevant policies including

- Cyber safety and Anti-Bullying Policy
- Acceptable use of Technology and the Internet
- Mobile Phone Policy
- Anti Bullying Policy
- Behaviour Management policy

……and report to the Principal who will investigate before applying the appropriate sanctions

4. Inform the sender's e-mail service provider
5. Notify parents of the children involved
6. Consider delivering a parent workshop for the school community
7. Consider informing the police depending on the severity or repetitious nature of offence
8. Inform DECS through the appropriate channels

Malicious or Threatening Comments Posted on an Internet site; about a pupil or member of staff.

1. Inform the site administrator of all suspected or known incidences of inappropriate comments posted on socially accessible domains. eg emails, blogs etc.
2. The site administrator will secure and preserve any evidence.
3. The Systems Administrator will look at the evidence and monitor the usage of ICT, where necessary action will be taken to trace the source and to stop abuse and prevent future occurrences.
4. The Police +/ DECS will be informed as appropriate.
5. Consider delivering a parent workshop for the school community „Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

1.9.1 Handling Cyber Safety Complaints

Prompt action will be required if a complaint is made.

The facts of the case will need to be established. For instance it is possible that an issue has arisen through home Internet use or by contacts outside school.

Transgressions of the rules by pupils could include minor as well as the potentially serious. The school's complaints / Grievance procedure will be used as appropriate and sanctions for irresponsible use must be linked to the school's behaviour policy.

In more serious situations the Police must be contacted.

Complaints of any Internet misuse will be dealt with by senior staff
Any complaint about staff misuse must be referred to the Principal.

Pupils and parents will be informed of the complaints procedure.

1.10 SMART Tips

S	M	A	R	T
•**Secret -** Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!	•**Meeting** someone you have contacted in cyberspace can be extremely dangerous. Only do so with your parent's/carer's permission, and only when they can be present.	•**Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages. They are not safe and should be deleted without opening	•**Remember** someone on-line may be lying and not be who he or she say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!	•**Tell** your parent or carer if someone or something makes you feel uncomfortable or worried

Figure 1-a SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees

1.11 Circular to Parents

Dear Parents,

As an important part of your child's education and in the development of ICT skills, The English language school is providing supervised access to the Internet. We believe that the use of the Internet is worthwhile and an essential skill for children as they grow up in the modern world. Please read carefully the attached Policy and Rules for Responsible use of technology (mobile phones, iPods, cameras, tabs etc), and Internet Use and discuss these with your child.

As there are concerns about students having possible access to in appropriate materials through the Internet, we are taking positive steps to deal with this risk in school. Our school operates an internet filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish.

At English language school we take the following steps to ensure an acceptable use of Technology including access to the Internet:

- Use of a filtered internet access.
- Supervised access and use of the internet by students.
- Websites used by the students will be chosen by staff prior to use.
- Regular checks of computer use logs including internet browser history, bookmarks and emails.
- Students will be informed of the attached Rules for Responsible Internet Use.
- Students should bring ICT devices from home with written parental consents and use will only occur after the content has been vetted bystaff.

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.

If you have any concerns regarding your child's use of the Internet in school then you are most welcome to contact the school for further information.

Yours Sincerely,

Principal

1.12 Internet Safety Rule for Students

- ✓ I will not look at, change or delete other people's work/files.
- ✓ I understand that I will not use gadgets inside or outside the classroom without my teacher's permission.
- ✓ I know that I am not allowed to use my gadget before morning assembly time, in the break time and after home time.
- ✓ I promise, I will not upload any picture or video taken in the school premises to social networking or other websites with teacher's permission.
- ✓ I will ask permission before entering any website, unless my teacher has already approved that site.
- ✓ I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and sensible.
- ✓ I understand not to provide my personal information on the internet.
- ✓ I understand that I am not allowed to open social media websites and chat while using gadgets in the school.
- ✓ 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 if I deliberately break these rules I could be stopped from using the Internet.

Pupil's Name & Signature	
Class	
Parents Signature	