

APPENDIX 17 – E-TECHNOLOGY

To be read in conjunction with the GB Taekwondo Safeguarding Children Policy and Procedures.

This policy is written to inform children and adults about how to stay safe online. There are some references to explicit behaviour and it is recommended that parents read it through before they share it with younger children.

INTRODUCTION

This document is to help protect young people who make use of technology whilst they're within the care of GB Taekwondo (GB TKD). It provides practical examples to protect information, ways to interact safely and how to create a better online community. Whilst the guidance is aimed at children and young people aged 11 and over, some of the language and types of things explained are not suitable for younger children.

Anyone aged under 13 should not be using social networking sites, such as Facebook, Instagram, Tumblr or Twitter, and to do so would be breaking the sites' rules and putting the user(s) at risk. Some sites require users to be older.

This policy applies equally to help all children, young people, athletes, staff, coaches and volunteers understand some of the key risks using online technology and the need to protect privacy.

Risks can include inappropriate:

- **Contact** - people who may want to cause harm, i.e. to bully, groom or abuse.
- **Content** - age-inappropriate or unreliable content that may be available.
- **Conduct** - putting yourself at risk through your own conduct, i.e. sharing too much.
- **Commercialism** - being unaware of hidden costs and chat, pop-ups, advertising in apps, games and websites.

This guidance supports GB TKD's safeguarding policy and it is important that all persons noted above including those working on behalf of GB TKD are aware of and follow this.

All staff and volunteers should ensure a clear differentiation between their personal and professional online profiles.

OVERVIEW

Sharing things, commenting, chatting and staying in touch with others is a great benefit of the internet. Social network sites however can be used to abuse information or situations, i.e. to share horrible comments or to bully people. **GB TKD has a zero-tolerance approach to bullying (see Appendix 2 – anti-bullying policy & graph).** It is important to understand how to use e-technology safely and know what the risks can be.

Things posted online can be seen by lots of people and can stay online forever. This is known as a **“digital footprint”**. It is a trail of information that people follow and can learn a lot from; these people may or may not be known to you. **“Footprints”** can show people at their best or their worst, and posts can have serious consequences.

Once you've read the information and advice below, why not test your knowledge with the “Safer Internet Day” quiz and see how much you know about staying safe online:

<http://www.saferinternet.org.uk/safer-internet-day/2015/things-to-do/quiz>

THINK BEFORE POSTING

Pause...take a moment to think about what you post to help prevent silly mistakes. For example, would you be happy to see what you post on an advertisement board, where your friends, parents, family, neighbours could see it? If not, think twice about sharing online!

APPENDIX 17 – E-TECHNOLOGY

As a general rule always consider:

- Am I commenting only about myself?
- Would I be happy for this comment to be quoted wider, i.e. in a newspaper?
- Will this comment reflect positively upon me, my sport, my team?

Things shared with friends as a joke may not be taken as a joke by others. Think about how content posted may be judged by others, i.e. would it impress a teacher, tutor or future employer, or could it cause offence? Will these people think positively of you, your sport, your team etc?

You can lose control of things shared online, even if you delete a photo or post. You can't guarantee what you share will not be copied or downloaded by someone else. Think about how many people you share information with. Will they take care of what you share or could they change it and share it without you knowing?!

A good example is shared in this link: https://www.youtube.com/watch?v=-f2QzoNb_C8 (part of the BBC's Horrible Histories series and features a comical clip on Guy Fawkes and internet privacy settings)!

How much should I share? The more you share, the more people learn about you. This can be used by some people in a negative way, i.e. to bully you, or to contact you and lie about liking the same things. Some people may set up fake profiles on social networks and can pretend to be a girl or boy your age when they're actually a lot older. It can be difficult to tell the difference between someone genuine and someone who is not.

A good example is shared in this NSPCC link "Lucy and the Boy: Be Share Aware": <https://www.youtube.com/watch?v=kwcl-VP3FYc&feature=youtu.be> In this animated clip, Lucy shares photos with someone she thought was a boy online.

Would I want this shared about me? Think about the impact of what you may post may have on others. Do you have your friend's permission to share funny pictures of them?

Remember, if you are worried, frightened or have any concerns regarding safety on line you can seek the support of an adult you trust, report to CEOP, or get help from any of the contacts below. Concerns can include someone using what you've posted online to harm you, asking you to meet up face to face, talk to you about things they shouldn't online or on webcam.

UNDERSTANDING WHAT PERSONAL INFORMATION MEANS

The following link is a clip from CEOP's "Thinkuknow" education programme (for 11-16 years) which helps to explain a need to be just as protective of personal information online as in the real world. It also directs where to go and what to do if young people are worried about any of the issues covered.

https://www.youtube.com/watch?feature=player_embedded&v=hK5OeGeudBM

SAFER SHARING AND SOCIAL NETWORKING

Privacy settings - Learn how to, and use, the privacy settings on the website, apps and social network sites you use. This will help you control what you share and with whom. You decide whether your friends, friends of friends or everyone can see what you post. It is advisable to only let people you know and trust see your information. Learn how to block people who are bothering you.

Choose your friends wisely - Share with friends you know in the real world! It is very easy to accept many friend requests or followers but remember they could be anyone. Remember too that what your friends share about you and their privacy settings online will also affect your "**digital footprint**".

Be a "good friend online" - This is about being kind, being supportive and reporting anything/anyone that upsets you/others online. Show respect for others online. Nasty behaviour online hurts just as much as unkind behaviour offline. Always treat others the same way you would like them to behave towards you.

APPENDIX 17 – E-TECHNOLOGY



Be supportive - Look out for your friends and family online and help others to use technology safely.

SHARING PHOTOS AND VIDEOS ONLINE

It can be hard and sometimes impossible to delete pictures or videos from the internet or other people's mobiles. Photos can easily be copied, changed, shared and used elsewhere so you need to make sure that pictures or videos are suitable for the internet. However, it is never too late to get help if you have shared something you regret.

Have I got permission? If you've taken a picture of someone else, have you got their permission to post it online? Could it upset or embarrass them? If you were them, would you be happy to share it? If you think the answer may be "no" then go and ask them, or don't post it at all.

Remember pictures of you (or others) in a uniform or in front of your sport club, for example, can identify where you hang out/identify you to a place.

Is it legal? Taking and sharing naked or "sexy" pictures or videos of people under 18 is illegal, even if you're taking them of yourself. You shouldn't also share naked or "sexy" pictures of other young people – this is illegal and can cause very serious problems for them.

LOST CONTROL

Remove and report - If you think you shouldn't have made a comment or posted a picture or video make sure you know how to remove anything you regret posting from the sites you use. There is support available on the services you're using. Report anything or anyone that upsets you or others online. Most websites will have a "safety centre" explaining how to do it. The fastest way to get it down is to remove it yourself. Log on to the site and delete it.

If someone else has posted it, ask them to take it down from the site. If they won't, speak to an adult you trust or someone in school, or see below for other advice and reporting options.

Report it to the website - If it's been posted on a popular website like Facebook or YouTube you can make a report to the site to ask them to take it down. Most sites have rules to stop people posting embarrassing or hurtful pictures – if the pictures or video breaks these rules they should delete it from the site.

GAMING

In common with sharing information on social networking sites you need to be careful when playing games and where you may have the ability to chat online in these games, making friends, with people you don't know. People can try to gain your trust and make you a friend for the wrong reasons. It is easy to lie online and some online friends can be adults who want to hurt you.

Be alert, look out for people trying to:

- build your trust by making you think they have things in common with you, for example hobbies.
- get you to add them on a social network or obtaining your personal details such as your phone number or photos, or to chat on a webcam. They may be wanting to ask things they shouldn't or ask you to do things you don't want to do.
- offer "cheats" to help you out with a game, trying to build you trust – think about why they are doing this. Are they a real friend?
- obtain information from you such as where you live and what school you go to. This is part of their attempt to get your trust – this tells them how to find you in the real world.

See below section "staying secure online" and be aware for example that if someone shares a link with you it could be a computer virus or spyware – don't click on links from people you don't know.

APPENDIX 17 – E-TECHNOLOGY

Play online games safely

Considering the points about being alert above, don't be fooled and think you know people you meet online.

- Don't tell them everything about yourself or chat anywhere else online with them, such as a social network site or a messaging app.
- Choose a username that doesn't reveal your identity or give away information about you, such as your name, nick name, age or date of birth, where you live or hometown. If you need to block anyone from bothering you, you have peace of mind that they can't find you again!
- Ensure your antivirus software and firewall are activated.
- Watch out for scams in computer games when buying or selling "property" – these can lead to being scammed by other users online.
- Keep your parents involved by letting them know what games you play - this helps them to understand what you like so much about them. It also helps them understand technology that they may not have grown up with and want to learn how to use, or they may be familiar with technology and be able to help with your settings!

Don't forget you can to an adult you trust or get help – see below contacts.

STAYING SECURE ONLINE

There are lots of ways people can try to steal personal information, therefore it is important to keep your information secure. You wouldn't leave the front door or window to your house open, neither should you leave your computer or phone unlocked! *Tip: to lock your computer/laptop screen press the "window symbol key" and the letter "L" – remember to set a password too!*

Set strong passwords - Use a different one for each site you use and make sure it's a mix of letters, numbers and symbols. Don't use easy to guess ones, like your date of birth or sequential numbers or letters. *Tip: Try using a mix of numbers, upper and lowercase letters and symbols!*

Check URLs - this is the address of a website and you can find this in the address bar at the top of the page. The URL for the official website of GB Taekwondo is <http://www.gbtaekwondo.co.uk/home.html>. When you click on a link you should always check the URL is the one you would expect for the site before you enter details.

Don't click on links from people you don't know - These could take you to sites that download viruses or harmful software onto your computer. Never enter details into a site you're not sure about, even if a link has come from a friend.

Always use antivirus software - If you've got your own computer make sure you get anti-virus software and keep this updated.

Keep your password to yourself - Never share, even with a best friend, or leave your phone or computer unlocked – this can expose it to access by others.

Top 5 crimes online:

- **Hackers:** people who try to break into your computers to steal information, files or cause trouble.
- **Phishing:** this is when criminals set up fake websites that look like real ones and send emails pretending to be from a bank saying they need your details. If you respond entering details they have your password etc and can take over your account.
- **Viruses and malware:** software that can mess up and infect your computer and delete files. Viruses can then spread to other computers often by email.
- **Ratting:** a remote access trojan – a trojan is software which is put on your computer without you knowing it, and means criminals can take control of your computer and spy on your files, delete stuff or even turn on your webcam!
- **Clickjacking:** criminals trying to get you to click on links that look interesting but download viruses etc. This could be for example, "click here to win a free ipod". Don't trust and click on links from people you don't recognise or that seem just too good to be actually true...they usually aren't!

APPENDIX 17 – E-TECHNOLOGY

CONTACTS

CEOP: The Child Exploitation and Online Protection Centre works across the UK tackling child sex abuse and providing advice for parents, young people and children.

Web: www.ceop.police.uk/safety-centre/

Report it: <https://www.ceop.police.uk/Ceop-Report/>

Childline: a free helpline for children and young people, where no problem is too big or too small.

Call: 0800 1111 (this number won't appear on your phone bill)

Web: www.childline.org.uk

You can also post messages and get advice on Childline's message board

Other people who can help are provided in this link and include the **Internet Watch Foundation** and **Action Fraud:** http://www.ceop.police.uk/safety-centre/other_reports/

GB Taekwondo Safeguarding Officers:

Mary Brownlow

Mobile: 07889 538 902

Email: safeguarding@gbtaekwondo.co.uk

Steve Green

Mobile: 07540 711788

Email: safeguarding@gbtaekwondo.co.uk

Need immediate help?

Call 999 or contact your local police.

NSPCC Child Protection Helpline: Tel: 0808 800 5000

Childline: Tel: 0800 1111

FURTHER INFORMATION

Further reference guides, education packs and information, many specific to age groups, is available at the below links:

<http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/>

Information to be "share aware", helping to keep your child stay safe on social networks, apps and games.

<https://thecpsu.org.uk/news/2015/january/keep-children-safe-online/>

The NSPCC's straightforward, no-nonsense advice to help parents keep their children safe online.

<https://www.getsafeonline.org/safeguarding-children/>

Plenty of policies, advice, checklists and resources to keep youngsters safe online and according to age group.

<http://www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx>

A multitude of information about online and mobile safety.

<http://www.saferinternet.org.uk/>

E-safety tips, advice and resources to help children and young people stay safe on the internet.

<http://www.thinkuknow.co.uk/>

The latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it. If you look after young people there's an area for you too – with resources you can use in the classroom or at home

APPENDIX 17 – E-TECHNOLOGY

<http://chatdanger.com/>

A site all about the potential dangers on interactive services online like chat, IM, online games, email and on mobiles.

Guidance developed using material from:

www.saferinternetday.org.uk,

<http://www.thinkuknow.co.uk/>

www.ceop.police.uk/safety-centre/

sjs: 03/06/15, updated 23/09/15 safeguarding contacts & other helplines