

ECB E–Safety Guidelines on Communication and Interactive Technologies

The internet, mobile phones, gaming, social networking and other interactive services have transformed the way in which we live. The new technologies offer tremendous opportunities to reach, communicate and engage with those involved in sport including members, supporters and players however as with any environment there are also risks.

The ECB is keen to promote the safe, and responsible, use of communication and interactive communication technologies within cricket. A blocking and banning approach, which merely limits exposure to risk, has been considered as no longer sustainable in many schools. Instead the focus is on empowering children with the skills and knowledge they need to use interactive communication technologies safely and manage the risk, wherever and whenever they go online. These ECB guidelines follow this empowerment approach to ensure the message of safe and responsible use of communication and interactive technologies is understood and guidelines are followed within cricket.

These guidelines provide the opportunity for all clubs to develop an e-safety acceptable use policy and review existing safeguarding policies and procedures to ensure online risks are managed and responsible use encouraged.

All clubs must read the guidelines below and create a policy from this guidance that is manageable within their own environments. An e-safety checklist to assist clubs is included.

Understanding the technology

Part of the challenge for many adults when considering safeguarding children and young people online is the gap between children's knowledge of the technology and their own general lack of understanding, knowledge and skills in relation to the online world.

Developing a basic knowledge of the technology used within your club can help staff, volunteer helpers and other members understand e-safety issues, manage risks and deal with incidents as well as supporting junior members and those parents/carers who seek advice and information.

The internet has evolved to become an increasingly dynamic and interactive medium led by social networking services. Thanks to the convergence of technical and communication platforms, services users can now interact with each other across multiple platforms and devices, such as mobile phones, personal digital assistants, games consoles and PCs. These services are very popular with children and young people.

In one sense, social networking is nothing new. These services, for the first time, simply bring together pre-existing interactive technologies on a single service. These technologies, and tools, can include all, or some, of the following: search, email, messaging, chat, blogs, gaming, discussion forums, Voice over Internet Protocol (VoIP), photos, music and videos.

Further information, including a selection of online guides for children, parents/carers and teaching professionals on the various technologies, including their benefits and risks, are available from the organisations listed below:

Childnet: provides a **Know It All guide**. (www.childnet.com)

Teach today provides a useful guide to the technologies.
(www.teachtoday.eu/en/technology-today/key-technologies.aspx)

The Child Exploitation and Online Protection Centre provides a guide to the technologies and education and awareness resources aimed at parents, children and young people and professionals - thinkuknow (www.thinkuknow.co.uk)

What are the potential risks to children and young people using new communication technologies, including interactive services?

With all emerging technologies there is the potential for misuse. Risks associated with user interactive services include: cyber bullying, grooming and potential abuse by online predators, identity theft and exposure to inappropriate content including self-harm, racist, hate and adult pornography.¹

Some of these risks can be a continuation of the risks children and young people experience offline and many children and young people also fail to realise that the internet is a public place.

It is crucial clubs, and those who have contact with children in cricket, understand e-safety issues and the potential risks to children and young people using new communication technologies, including interactive services to be able to fulfil the club's duty of care, safeguarding role and responsibilities.

The Byron Review sets out risks to children posed by the internet and illustrated by the following grid.²

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

¹ EU Kids Online: Comparing Children's Online Activities and Risks across Europe: Hasenbrink, Livingstone, Haddon, Kirwil and Ponte, 2007. Available at : www.eukidsonline.net

² The risks children and young people face from the internet and video games were subject to an independent review during 2008 and the government has set up the UK Council to take forward the recommendations of the "Safer Children in a Digital World: the Report of the Byron Review". See Byron Review <http://www.dcsf.gov.uk/byronreview/2007>

Most children and young people use internet positively but sometimes behave in ways that may place themselves at risk. Some risks do not necessarily arise from the technology itself but result from offline behaviours that are extended into the online world, and vice versa.

Potential risks can include, but are not limited to³:

- Bullying by peers and people they consider ‘friends’
- Posting personal information that can identify and locate a child offline
- Sexual grooming, luring, exploitation and abuse contact with strangers
- Exposure to inappropriate and/or illegal content
- Involvement in making or distributing illegal or inappropriate content
- Theft of personal information
- Exposure to information and interaction with others who encourage self harm
- Exposure to racist or hate material
- Encouragement of violent behaviour, such as ‘happy slapping’
- Glorifying activities such as drug taking or excessive drinking
- Physical harm to young people in making video content, such as enacting and imitating stunts and risk taking activities
- Leaving and running away from home as a result of contacts made online

Potential indicators of online grooming and sexual exploitation of children and young people

There is also concern that the capabilities of social networking services may increase the potential for sexual exploitation of children and young people.

Exploitation can include exposure to harmful content, including adult pornography and illegal images of child sexual abuse also referred to as indecent images. There have also been a number of cases where adults have used social networking and user interactive services as a means of grooming children and young people for sexual abuse.

Online grooming techniques include⁴:

- Gathering personal details, such as age, name, address, mobile number, name of school and photographs
- Promising meetings with sports idols or celebrities or offers of merchandise
- Offering cheap tickets to sporting or music events
- Offering material gifts including electronic games, music or software

³ Ref: Home Office Task Force on Child Protection and the Internet: Good practice guidelines for the providers of social networking and other user interactive services 2008. See UKCCIS <http://www.dcsf.gov.uk/ukccis/>

⁴ For further information on sexual exploitation of children and young people online see the Home Office Task Force on Child Protection and the Internet: Good practice guidelines for the providers of social networking and other user interactive services 2008. See UKCCIS. <http://www.dcsf.gov.uk/ukccis/>

- Paying young people to appear naked and perform sexual acts
- Bullying and intimidating behaviour, such as threatening to expose the child by contacting their parents to inform them of their child's communications or postings on a social networking site, and/or saying they know where the child lives, plays sport, or goes to school
- Asking sexually themed questions, such as 'Do you have a boyfriend?' or 'Are you a virgin?'
- Asking to meet children and young people offline
- Sending sexually themed images to a child, depicting adult content or the abuse of other children
- Masquerading as a minor or assuming a false identity on a social networking site to deceive a child
- Using school or hobby sites (including sports) to gather information about a child's interests likes and dislikes. Most social networking sites set a child's webpage/profile to private by default to reduce the risk of personal information being shared in a public area of the site

For further information including the latest news and updates on sexual exploitation online visit the Child Exploitation and Online Protection Centre, a UK law enforcement agency dedicated to tackling sexual exploitation of children, including the offline environment. (www.ceop.gov.uk)

Reviewing your safeguarding policies

Looking at online safety issues provides the opportunity to review your club's existing safeguarding policies.

E-safety is an important part of safeguarding rather than an isolated issue therefore the club's designated Welfare Officer is best placed to ensure the club is adopting, and implementing, the e-safety policy and be the "first point of contact" as set out in the ECB Guidance on Appointing and Training a Club Welfare Officer.

Ensure your existing safeguarding policies and procedures address safeguarding children online, including dealing with e-safety incidents and where to report concerns.

This should include:

- The potential risks and indicators of online grooming and sexual exploitation of children and young people. These should be reviewed on a regular basis in light of incidents dealt with by the club and cases known to law enforcement. See section on potential risks
- Procedures for the reporting of potentially illegal/abusive content or activity, including child sexual abusive images and online grooming concerns arising online should be reported as follows:
 - Illegal sexual child abuse images should be reported to the Internet Watch Foundation (<http://www.iwf.org.uk>) and to the police.
 - Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre (www.ceop.gov.uk). Law enforcement agencies and the service provider may need to take urgent steps to locate the child and/or remove the content from the internet.

- Where potentially illegal material including sexual abuse or indecent images of children or activity is found or suspected on technology provided by, or where the club has access to, the evidence should be made secure and preserved. The police or the IWF can provide further advice on this when a report is made. In the case of reports about suspected illegal material including sexual abuse or indecent images of children held on personally owned devices by members the report should include where the suspected illegal material can be found e.g. a website address where possible. Website addresses can be found in the web browser window
- Potentially illegal material, including sexual abuse or indecent images, should not be circulated or distributed within the club. Those involved in making a report should be kept to an absolute minimum. Ideally this should be the Club Welfare Officer

Where a child or young person may be in immediate danger, always dial 999 for police assistance.

Cyber-bullying

Cyber-bullying is a form of bullying and clubs should address cyber-bullying as part of their existing anti-bullying policies.

Responding to cyber-bullying should include⁵:

Supporting the person being bullied

- Give reassurance that the person has done the right thing by telling someone. Refer to any existing pastoral support/procedures and, where it is a junior member, inform parents
- Make sure the person knows not to retaliate or return the message
- Help the person to keep relevant evidence for any investigation (e.g. by not deleting messages they've received, and by screen capture shots and noting web addresses of online cyber-bullying instances)
- Check the person understands simple ways to prevent it happening again e.g. by blocking contact

Take action to contain the incident

- If you know who the person responsible is, ask them to remove the content
- Contact the host (e.g. the social networking site) to make a report to get the content taken down

For further information see Government guidance for schools *Safe to learn: Cyberbullying: a whole-school community issue* (www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying)

Beatbullying and its cybermentors programme provide support and advice to children and young people. (www.beatbullying.org) and (cybermentors.org.uk)

⁵ Childnet advice

Encouraging safe and responsible use

Encouraging safe and responsible use of communication technologies by all those involved in the club's activities is a key part of a club's e-safety and acceptable use policies. Many internet, mobile, social networking and other interactive services provide safety warnings and advice including videos and links to online safety.

Ensure club staff and volunteers are aware of online risks and the need to protect their own privacy online. They should understand the risks in posting, and sharing, content which may damage their reputation within the cricket environment.

Safe and responsible use includes:

- Adhering to terms of service and acceptable use policies
- The importance of children registering on social networking sites with the correct age. Depending upon the service this can ensure safety settings are appropriately applied, only age appropriate advertising is available and a child's profile is not subject to an online search. The minimum age for most social networking services is 13 yrs of age
- Use of privacy and safety settings – these enable users to manage 'who sees what' and who the user wishes to interact and share photos and other information with
- 'Think before you post' content including messages, videos and photos

Teachtoday is a unique collaboration of the ICT industry and offers links to the safety and privacy advice provided by the major internet service providers, mobile operators and social networking services.(www.teachtoday.eu)

Following the establishment of the UK Council for Child Internet Safety (www.dcsf.gov.uk/ukccis) the Government launched the cleverclickclicksafe e-safety code campaign in February 2010 (clickcleverclicksafe.direct.gov.uk).

Guidelines on creating and using an acceptable use policy

The ECB is keen to promote the safe and responsible use of communication and interactive technologies within cricket. These guidelines provide the opportunity for all clubs to develop an e-safety acceptable use policy. An acceptable use policy is the common term used in schools to set out what is acceptable and unacceptable behaviour online and is similar to a code of conduct.

Each club will be different in set up and facility access which is why each club must create their own policy. A photocopy of this page is not a club policy.

All clubs must read the guidelines below and create an e-safety acceptable use policy from this guidance that is manageable within their own environments.

Clubs must create an e-safety acceptable use policy relating to the use of communication and interactive technologies. This should include fixed and mobile internet (PCs, laptops, webcams and digital video equipment, technology provided by the club or where the club has access to, personally owned devices and use of, by members including junior members, staff, volunteer

helpers and guests on club premises, during home and away matches, training sessions, on tour, or within the context of cricket online). The club's existing code of conduct may be a useful starting point.

The guiding principles are:

All members and guests of this Club will:

- Take responsibility for their own use of communication and interactive technologies, making sure they use new technologies safely, responsibly and legally within the context of cricket
- No communication device or service, including interactive communication services such as social networking may be used to bring the club, its members or cricket into disrepute
- No communication device or service, including interactive services such as social networking may be used for inappropriate behaviour online within the context of cricket including the bullying or harassment of others in any form, defamation, obscene or abusive language, the uploading of material which is libellous, defamatory, obscene, illegal, shows nudity or is violent
- Report any known misuses of communication and interactive technologies within the context of cricket, including unacceptable behaviour, inappropriate contact with children online and illegal content including sexual abuse/indecent images of children, according to the relevant club and ECB safeguarding policies and procedures
- Need to be aware that any report of the misuse of communication and interactive technologies within the context of cricket will be investigated according to the club's policy and procedures and may result in the club's sanctions being enforced. Depending upon the seriousness of the incident legal action may be taken and where suspected criminal activity has taken place a report will be made to the police

Where a club provides network access or communication devices all members and guests will:

- Protect passwords and personal network logins and log off the network when leaving web stations/devices unattended. Where available security settings should be set on mobile devices. Any attempts to access, corrupt or destroy other users' data in any way using technology is unacceptable

In addition to the above club officers and appointed volunteers will:

- Take responsibility for their professional reputation in the online environment, making sure they follow e-safety advice, adhere to privacy and safety settings and report any concerns in accordance with club and ECB policies and procedures
- Not ask for email addresses, mobile phone numbers or social networking profiles of junior members (less than 18 years of age) or search for junior members on social networking services/search engines without the prior consent of parents and in line with the club's policy on the use of information including emergency situations

- Not develop an online relationship with a young player with the intention of meeting them offline to engage in sexual activity. Sexual exploitation, including grooming a child under the age of 16 for the purpose of meeting to engage in sexual activity, is a serious criminal offence
- Not view, possess, make or distribute sexual abuse/indecent images of children. This is a serious criminal offence

For further information on acceptable use policies:

BECTA have produced a range of acceptable user policies (publications.becta.org.uk/display.cfm?resID=25934)

Is your club e-safe?

Does your club.....

- Welfare Officer understand e-safety issues?
- have safeguarding policy and procedures which addresses online issues? This should include, dealing with e-safety incidents such as cyber-bullying, inappropriate content and potentially illegal images of children
- have an acceptable use policy for interactive communication technologies? This should state what is acceptable and unacceptable behaviour when using communication technologies within the context of cricket
- raise awareness of e-safety to all members and parents?
- request confirmation from parents/carers that the club's e-safety policy has been read, or parents/carers are aware of the club's e-safety policy? See Player Profile/Parental Consent Forms

Do all your club staff and volunteer helpers.....

- understand e-safety issues and risks?
- know where to direct junior members and their parents to sources of advice and information about e-safety?
- know how to report and manage issues or concerns?
- know how to keep data safe and secure? This should include the personal contact data of other club members such as mobile phone numbers, email addresses and social networking profiles
- know how to conduct themselves appropriately when using interactive communication technologies and protect their reputation online within the cricket context?
- take the opportunity to consult with junior members about e-safety issues and in relation to the club's policies?

Do your junior members.....

- understand what online safe and responsible use means within the cricket context?
- understand the risks and assess the potential risks of using any particular technology and behave safely and responsibly to limit those risks?
- know where to go for advice and information about e- safety?
- get the opportunity to give their views about staying safe online?
- know how to report any concerns they may have?

Can you help members and carers of junior members.....

- understand e-safety and manage risks?
- understand their roles and responsibilities?
- keep up to date with advice on e-safety?
- know how to report any concerns they may have?



Using social media: e-safety guidelines

The new technologies offer tremendous opportunities to reach, communicate and engage with those involved in sport including members, supporters and players in a creative medium where users are active participants. This is sometimes called social media. These guidelines specifically target the following people in your club:

- The lead officer responsible for promoting sporting opportunities
- The Welfare Officer
- Communication and/or marketing person
- IT manager and/or web master

These are the key people who will be involved in taking forward your club's involvement in social media and they will need to work together to ensure the necessary safeguarding measures are in place and followed on a day-to day basis.

Your club may be considering, or already using, social media to involve members, including children and young people in activities and gain their participation in virally dissipating information or campaign messages about a cricket event. It is most likely that many supporters of cricket around the world are already initiating discussions about cricket in blogs, forums, and groups and uploading their favourite cricket clips onto their profile to share with others.

Social media generally uses existing social networking services and examples of popular services include: Bebo, Facebook, Flickr, Piczo, MySpace and Twitter and video sharing sites such as YouTube.

These guidelines on using social media should be viewed as part of the ECB guidelines on e-safety and build upon the club's acceptable use policy. These ECB guidelines are developed from the NSPCC CPSU Briefing: Using Social Networking and Social Media: Promoting Safe and Responsible Use.

Follow your Club's Acceptable Use Policy

Your club's acceptable use policy should contain some key safety principles about acceptable and unacceptable behaviour. Safety and privacy tools are a useful place to start. Take time to become familiar with safety aspects of interactive communication technologies and the specific service the club intends to use, including the minimum registration age, terms of service and where to report concerns **before** setting up a club profile.

Ensure the key people involved in setting up and managing your club's online presence understand the potential risks to children and young people online and know how to deal with e-safety incidents including where to report concerns. See ECB E-Safety Guidelines on Communication and Interactive Technologies.

Ensure club members and others are aware of your club's acceptable use policy and how it relates to their interaction with the club's profile. If your club has just set up a profile on a social networking service this provides an opportunity to promote your club's acceptable use policy.

Managing your club's presence online – ensuring e-safety

You will need to decide who will have responsibility for the setting up of the club's presence online including the profile if it is a social networking service. Key areas to consider include:

- *The target audience* – is it clear who the interactive service or profile, if it's on a social networking service, is targeting. Is it aimed at adult or junior members, or both? If access is restricted to adult members of the club how is this monitored? Is this communicated to members and is it clear when registering on the service? Most social networking services have a minimum registration age of 13 set by US law
- *Content* - is the content you wish to upload appropriate for the intended audience? Does it fit within your club's acceptable use policy on acceptable behaviour and legal content? Who deals with unacceptable behaviour and illegal content posted by users?
- *Interaction with others and moderation* - if there is interaction with other users, for example in a forum area, who has responsibility to moderate discussion, encourage acceptable behaviour and enforce the acceptable use policy? Will other users be able to post comments before being reviewed?
- *Contacting the service and reporting concerns* - is there a contact facility on the website or interactive service for users to contact or report a concern? If your club is setting up its own interactive service who will handle the reports made to the website and is the report facility checked on a regular basis?
- *Safety and privacy tools* – many social networking services provide safety and privacy tools to enable users to manage their interaction with others including reviewing comments and messages from other users before they appear on your profile. Your club should consider utilising these safety and privacy settings and also reviewing them on a regular basis as service providers often update these facilities

For further information on good practice guidance on web based services, instant messaging, chat, moderation, safer search and social networking services see the Home Office Child Protection and the Internet Task Force guidelines.

Fake or imposter profiles on social networking services

Beware of fake, or imposter, profiles of well known sports or celebrity people. It has been known for fake, or imposter, profiles to be set up on social networking services. Sometimes this is intended to be fun, however, fake profiles can be set up by those with malicious intent to ridicule and harass. It can also be used to groom children by those seeking to gain a child's trust and then attempt to meet them offline. Always check with a club or the ECB offline before adding or promoting a profile in the name of a well known sports person to your club's profile or interactive service.

Avoid taking personal details of children online

Avoid asking children to divulge personal details online including home and email address, name of school, mobile numbers and so on. If you are promoting an event online it is best to provide details of the event and then direct users to where they can obtain further information offline. Personal details required for entry into competitions should comply with your club's

policies on information including legal requirements for data protection and guidance from the Information Commissioner in relation to children and young people.

Ensure staff, volunteer helpers and coaches are aware of the need to protect their own privacy online

Make sure club staff, volunteer helpers and coaches are aware of the need to protect their privacy online. They should understand the risks in posting and sharing content which may damage their reputation. Links and contact set up for the club, within the context of cricket in the online environment, should only be set up by those with responsibility to manage the club's presence online.

Include your club's contact details

Information about how to contact your club offline as well as a web address should be included together with any information on membership. This allows users to contact your organisation directly and verify your club offline.

For further information

The NSPCC Child Protection in Sport Unit guidance *Social Networking services, social media and sport: guidelines for safeguarding children and young people* (www.nspcc.org.uk/Inform/cpsu/resources/briefings/social_networking_services_wdf69029.pdf) provides further detail on social networking services and social media, and is a useful guide for setting up an online presence. It also helps with the safety implications for children and young people, your staff and organisation as well as providing further detail on social networking services and social media.

Home Office Task Force on Child Protection and the Internet on Chat, Instant messaging, Web- Based services, Moderation, Safe search and social networking services. Available on the UKCISS website: (www.dcsf.gov.uk/ukccis)

"Keeping your personal information personal" – a guide to the Data Protection Act 1998 for Youth, including the use of social networking services. (www.ico.gov.uk)