Appendix 12
Communications Policy

SOCIAL MEDIA

The use of social media provides staff and volunteers with a unique opportunity to engage and connect with colleagues and online communities. It enables them to disseminate information and good news stories about Association programmes and to share their passion for football in Northern Ireland.

POTENTIAL RISKS TO CHILDREN AND YOUNG PEOPLE

As with all emerging technologies, there is also the potential for misuse of social media. Risks associated with user-interactive services include: cyber bullying; grooming and potential abuse by online predators; identity theft; and exposure to inappropriate content, e.g. adult pornography, racist or violent content and self harm / pro-ana (pro anorexia) sites.

Most children and young people use the 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 to:

- Bullying by peers and people they consider 'friends'
- Posting personal information that could allow others to identify and / or locate a child offline
- Sexual grooming, luring, exploitation and abuse through contact with strangers
- Exposure to inappropriate content
- Involvement in making or distributing illegal or inappropriate content
- Theft of personal information
- Exposure to information about and interaction with others who encourage self harm
- Exposure to racist or hate material
- Encouragement of violent behaviour, such as 'happy slapping'
- Exposure to content 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 risky activities
- Leaving or 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 child abuse 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 include:

- Gathering personal details – name, address, mobile number, name of school and photographs
- Promising meetings with sports idols or celebrities, or offering merchandise
- Offering cheap tickets to sporting or music events
- Offering material gifts, including electronic games, music or software
- Paying young people to appear naked and perform sexual acts
- Bullying and intimidating behaviour, such as threatening to expose the child by informing their parents about 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-related ones) 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.

SOCIAL-NETWORKING POLICY

Staff and volunteers who use social media as part of their programme development are required to familiarise themselves with the potential risks which social media can bring to children and young people, and take all possible steps to minimise risks to children and young people. Staff and volunteers are required to fully adhere to the codes of conduct pertaining to social media use. Any breaches of the code may result in disciplinary action being taken.

CODE OF CONDUCT FOR STAFF AND VOLUNTEERS USING SOCIAL MEDIA WITHIN IRISH FA PROGRAMMES

The following guidance applies to all forms of social media platforms

- Before engaging in social media use, staff and volunteers are required to seek permission from their line manager and to inform the Director of Football Development and the Child Welfare Department of their intentions.
- All social media accounts must be set up using an official Irish FA address, and never a personal one, in order to reduce the risk of the establishment of impostor or fake profiles.
- Staff and volunteers who use social media assume overall responsibility for managing and moderating their accounts. However line managers have a responsibility to police such accounts to ensure that all content is appropriate and in line with Association policies.
- Staff and volunteers have a responsibility to familiarise themselves with safety aspects pertaining to social media use – this includes awareness of what is considered acceptable and unacceptable behaviour as an employee / volunteer on a social-networking service.
- Staff and volunteers must keep abreast of current legislation and good practice guidance pertaining to social media companies and adhere to all relevant legislation relating to communications, e.g. Communications Act 2003, Malicious Communications Act 1998 etc.
- Staff and volunteers must be aware of how this policy feeds into other policies outlined in this document, i.e. the Equality and Anti-bullying Policies and the Reporting Procedures.
- Staff and volunteers have a legal and moral duty to respond to any indications that illegal activity (e.g. grooming for abuse) is taking place by informing the Child Welfare Department, who will refer the concern on to the relevant statutory agencies and service providers.

Staff and volunteers must:

- use their social-networking page as a communications platform only – mainly to communicate on a generic basis with parents and guardians and children and young people, e.g. 'training has been cancelled tonight due to adverse weather conditions'
- ensure that the highest privacy and security settings remain activated at all times
- activate all swear filters in order to block any foul language from being disseminated to users

- where possible, monitor and view all written and visual content before accepting and posting it live
- delete and remove any inappropriate written content or images that would compromise the welfare of children and young people and / or the ethos of the Association
- be safety-conscious when adding content to an Association webpage / profile
- obtain written parental / guardian consent before posting pictures of children and young people who engage in Association activities
- communicate to third parties (i.e. spectators or venues) that it is their responsibility to obtain parental / guardian consent before passing on images of club activities to Association staff to be posted on social-networking sites. The Irish FA will not be held liable for third party actions.
- ensure, if using Facebook, that they only communicate with children over the age of 13 (in line with network providers guidelines), always through an official site, and that communication relates directly to Association activities (e.g. training / matches)
- not accept children or young people, who they are in a position of responsibility for during Irish FA programmes, as friends on their personal social-networking site
- respond to online bullying and report it to their line manager - what is said online should be treated as if said in real time
- never post any written or visual material that compromises the ethos and values of the Association
- post factual comments only. Do not enter into a debate regarding a match result etc.
- display details of their social-networking page on the Irish FA website so that children / young people and parents / guardians know that it is an authentic Association forum
- promote safe and responsible use of social media
- promote the safeguarding page and sign post users to this so that they can obtain links to the Child Exploitation and Online Protection Agency (CEOP)
- maintain professionalism at all times
- adhere to all best practice guidelines, as outlined in this document

Staff and volunteers must never:

- become friends via their own social media account with young people for whom they are in a position of responsibility
- communicate or share images via their personal social-network account with children and young people involved in Association programmes
- post any written or visual material that compromises the ethos and values of the Association
- engage in inappropriate communication with children and young people
- engage in grooming behaviour or behaviour that could be misconstrued as grooming
- engage in bullying behaviour on social-networking sites
- ridicule a child or young person by posting video images, whether intentionally or not. What may be funny to you may not be funny to others.
- use foul, abusive, sectarian, racist, discriminatory or sexualised language
- comment on indivi dual players

Remember:

Think before you post.

If you wouldn't say it in front of your mother or granny, then don't post it!

All comments on Irish FA social-networking sites will be considered as public comment and will be treated as such. The Irish FA therefore reserves the right to take disciplinary action in cases involving social-networking where the welfare of a child or young person is compromised or where the actions of a staff member / volunteer bring the Association into disrepute.

E-MAILING AND TEXTING

Emailing and text messaging are convenient and effective ways for staff to communicate with children and young people involved in Association activities. However, it is important that we consider potential risks to both parties:

Potential risks for children and young people include:

- inappropriate access to, or use or sharing of, personal details (e.g. name, email address, mobile phone number)
- unwanted contact by adults with malicious intent
- bullying by peers
- being sent offensive or inappropriate materials
- grooming for sexual abuse via personal communication
- direct contact and actual abuse

Potential risks for staff include:

- misinterpretation of their communication with children and young people
- potential investigation (either internal or by statutory agencies)
- potential disciplinary action

E-mailing and Texting Policy

- Where possible, staff should communicate information regarding programmes, events, training and matches through parents and guardians
- When updating children and young people, messages should be communicated in bundles and should be one-way. Written parental or guardian consent must be obtained before communicating messages directly to children and young people. Children and young people should only message back to acknowledge receipt of the message or for clarification. Staff have a responsibility to advise children and young people of this in advance. Parents and guardians should be presented with the option of being sent a copy of the message.
- Messages must never contain inappropriate, abusive or offensive material
- Direct communication with children and young people must only take place if absolutely necessary; it should be kept minimal and relate to Association activities only. In the event that a staff member is required to communicate directly with a child or young person, it is only appropriate if written parental / guardian consent has been obtained and the parent / guardian is informed in advance of what the conversation will relate to. The parent / guardian should also be sent a copy of the message that is being sent to their child. Where possible, however, direct communication with a player should take the form of a meeting in the presence of a parent or guardian – particularly if in relation to non-selection or behavioural issues.
- Only full-time staff should have access to players' mobile numbers and e-mail addresses.

Personal details pertaining to each child or young person must be stored in a secure cabinet or on an electronic system that is password protected. Access to such details should be kept to an absolute minimum. Permission to retain details should be obtained from both parents and guardians and also children and young people.

The Irish FA will follow disciplinary procedures should breaches of this protocol regarding messaging be broken.

The Irish FA recognises its legal and moral duty to consult with relevant statutory agencies should indications of illegal activity (e.g. grooming for abuse) come to light.