E-Safety Policy

Index Code	JFA – ES1
Author	Tim Pryor
Authorised By	David Kennedy
Issue Date	May 2020
Review Date	May 2021
Last Review Date	New Document
Changes	-
Overview	This policy is to ensure staff and volunteers use devices such as mobile phones, digital cameras, computers and other technology safely for communication and data storage purposes.

Document Index

1. Scope

1.1 This policy is to ensure staff and volunteers use devices such as, but not restricted to, mobile phones, digital cameras, computers and other technology safely for communication and data storage purposes.

1.2 The policy details the actions and behaviours that are required from staff and volunteers in order to maintain an e-safe environment.

1.3 The policy sets out recommended means of communicating with young people.

2. Personnel Responsible for Implementing the Policy

2.1 It is the responsibility of the Jersey FA E-Safety Officer to ensure staff and volunteers are aware of this policy.

2.2 The Jersey FA e-safety officer is the Marketing, Communications and Events Manager.

3. Compliance with Related Policies and Agreements

3.1 This policy should be used and read alongside the Jersey FA Social Media Policy and the Staff Handbook.

4. Device Security

4.1 All computer and mobile devices used for Jersey FA activity should be password protected.

4.2 Passwords should never be shared with anyone else.

4.3 All screens should be locked if devices are left unattended for any length of time.

4.4 Laptops may be used, and FA services may be accessed, outside of the Jersey FA network for example at home or in a library. However, laptops should always be connected via the FA's VPN service.

4.5 Staff and volunteers should not send or display material that is pornographic or that some people may find offensive (including emails, text messages, video clips and images sent by mobile phone or posted on the internet).

4.6 Apps and programmes should not be downloaded to FA managed devices without permission from FA IT.

4.7 Lost or damaged devices containing Jersey FA data should be reported to the CEO and E-Safety Officer immediately.

5. Data Storage

5.1 Data and other information about individuals held by the Jersey FA should only be accessible to staff and volunteers who need the information in the course of their work.

5.2 Data should be password protected and print outs should not be left unattended.

6. Email

6.1 Jersey FA email systems should primarily be for business use, although some personal usage is permitted.

6.2 Staff and volunteers should not allow other people to access their email account or to send emails from an account which is not their own.

7. Communication with Children via Technology

7.1 The following policy area relates to communication via technology including, but not restricted to, emails, text messages and mobile messaging services such as WhatsApp.

7.2 Staff and volunteers should preferably email or phone the child's parent or guardian rather than the child, if available using the contact details provided on sign-up forms.

7.3 Staff and volunteers should get signed consent from parent or guardian before communicating digitally with children. The purpose and method of communication should be agreed, and the parent or guardian should be copied in. Such communications should only be in relation to specific Jersey FA related activities, e.g. changes in travel arrangements or training times.

7.4 Jersey FA staff and volunteers should not spend excessive time alone with children away from others. In the "technological world" staff and volunteers should spend NO time alone with children.

7.5 Staff and volunteers should not give out their mobile number to children or seek a child's number.

7.6 Staff should not accept any personal friend requests on social media from any young person under their care.

7.7 Staff should not send out any personal friend requests on social media to young people under their care.

7.8 Personal social networking sites should not be used to contact young people within Jersey FA's care.

7.9 Staff should not put anything on social media that identifies a child, without permission from a parent or guardian.

8. Photography of Children

8.1 Photos and videos of children in the Jersey FA's care should not be taken without parental or guardian consent.

8.2 Photos and videos of children should not be shared or used publicly, online or in printed material, without parental or guardian permission.

8.3 Careful thought must always be given to who is able to access such photographs and videos.

8.4 Photographs and videos of young people should not routinely be accompanied by personal data, including the full names of those portrayed.

9. Social Media

9.1 For policy on Social Media please read the Jersey FA's Social Media Policy.

9.2 Staff and volunteers should only use social media for business purposes when given specific approval by the CEO or E-Safety Officer.

9.3 Occasional personal use of social media during working hours is permitted, at the discretion of the CEO, so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

9.4 Staff and volunteers must not use social media to make direct contact with children or young people known through football.

10. Using Phones Around Children

10.1 Staff should not use their phones around children, except for business and emergencies.

10.2 Staff should not take photos of children for personal use, for example on personal social media channels.

11. Monitoring and Review

11.1 This Jersey FA Policy will be ratified by the Board and will be reviewed annually. The date the Policy is ratified should be recorded in the respective Jersey FA Board minutes.

11.2 All incidents and near misses must be reported to the Jersey FA CEO and E-Safety Officer.

11.3 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, is continually monitored. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

12. Breach of this Policy

12.1 Breach of this policy may result in disciplinary action up to and including dismissal or, if a volunteer, you may be asked to stop volunteering for us. Any member of staff or volunteer suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.