MILTON KEYNES DONS FC

E-SAFETY POLICY.

AUTHOR	JOHN COVE
ROLE IN ORGANISATION	DIRECTOR / SENIOR SAFEGUARDING MANAGER
DATE OF APPROVAL	MAY 2020
DATE FOR REVIEW	JUNE 2021

INTRODUCTION

MK Dons Football Club recognises the benefits and opportunities which new technologies offer to enhance learning We encourage the use of technology in order to learn new skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are aware of potential risks and challenges associated with such use. Our approach is to implement safeguards and to support staff and participants to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard those we work with we will do all that we can to make our participants and staff stay e-safe and to satisfy our wider duty of care. This E-safety policy should be read in conjunction with other relevant policies.

PURPOSE

By following this policy and receiving appropriate training, people representing the Football Club will:

- be able to identify potential risks in their working environment and mitigate against these risks
- identify the different risks which young people and adults at risk might be exposed to through use of technology and know the signs which might suggest a participant is in danger
- be able to respond appropriately to allegations and concerns
- understand the roles and responsibilities of other professionals and know what to do if they are concerned about the actions others have taken.

Leaders with the Football Club will:

· monitor the implication of this policy

· arrange and mandate regular training for all staff, which is appropriate to their role and responsibility

· ensure lessons are learnt through their own regular evaluations and feedback from other agencies

· respond to any concerns promptly which implicate Football Club staff or volunteers

E-SAFETY RISKS

his policy identifies the risks and details the strategies involved in minimising E- Safety risks.
Guidance on dealing with youth produce sexual imagery can be found in Appendix 1 of this policy.

Examples of E-Safety Content

· Exposure to age-inappropriate material

· Exposure to inaccurate or misleading information

· Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance

· Exposure to illegal material, such as images of child abuse

· Exposure to extremist or radical views /materials

Examples of E-Safety Contact

· Grooming using communication technologies, leading to sexual assault and/or child prostitution

· Grooming using extremist or radical views/materials for the purpose of illegal activity

Examples of E-Safety Commerce

· Exposure of minors to inappropriate commercial advertising

· Exposure to online gambling services

· Commercial and financial scams

Examples of E-Safety Culture

· Bullying via websites, mobile phones or other forms of communication device

· Downloading of copyrighted materials e.g. music and films

POLICY SCOPE

The policy applies to all members of staff, volunteers and participants who have access to the MK Dons Football Club IT systems; both on the premises and remotely. The E-Safety Policy applies to all use of the internet and electronic communication devices such as e-mail, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information. It should also be read alongside the Football Club's Data Protection Policy.

ROLES & RESPONSIBILITIES

Safeguarding is everybody's business at MK Dons Football Club. There are clear lines of responsibility for reporting concerns regarding safeguarding within MK Dons Football Club. The first point of contact should be the Designated Safeguarding Officer. All staff & volunteers are responsible for ensuring the safety of participants and should report any concerns immediately to their line manager. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All participants must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be a Designated Safeguarding Officer. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Designated Safeguarding Officer may be asked to intervene with appropriate additional support from external agencies.

SECURITY

MK Dons Football Club will do all that it can to make sure the network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of systems and information. Digital communications, including email and internet postings, over the network, will be monitored.

Personal electronic equipment, e.g. phones, laptops, ipads etc. must not be used to hold or transmit personal data of anyone related to the business without the express permission of the Executive Director and the IT department. Failure to adhere to this may be considered Gross Misconduct.

BEHAVIOUR

MK Dons Football Club will ensure that all users of technologies adhere to the standard of behaviour as Football Club out in the Staff Handbook or in the case of the participant in the learner agreement. MK Dons Football Club will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and volunteers should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the participant and staff disciplinary policies and procedures.

Where conduct is found to be unacceptable MK Dons Football Club will deal with the matter via internal disciplinary procedures as described in the staff handbook. Where conduct is considered illegal MK Dons Football Club will report the matter to the police.

USE OF IMAGES AND VIDEO

The use of images, or photographs, is an integral element to some learning programmes and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or participants.

All participants and staff should be aware of the risks in downloading these images as well as posting them online and sharing them with others. There are particular risks where personal images are posted onto social networking sites, for example.

PERSONAL INFORMATION

Personal information is information about a particular living person. MK Dons Football Club collects and stores the personal information of participants and staff regularly e.g. names, dates of birth, email addresses and information regarding participation. This information is stored in accordance with the MK Dons Data Protection Policy and the latest data protection legislation.

Staff must keep participants personal information safe and secure at all times. When using an online platform, all personal information must be password protected. No personal information of individuals is permitted offsite unless the member of staff has the permission of their Line Manager.

All personal information must be stored on centralised systems and where possible secured by password or encryption.

EDUCATION AND TRAINING

With the current unlimited nature of internet access, it is impossible for MK Dons Football Club to eliminate all risks for staff, volunteers and participants. It is our view therefore, that MK Dons Football Club should support staff, volunteers and participants through training and signposting. This will provide them with the skills to be able to identify risks independently and manage them effectively. Staff, volunteers and participants should be signposted to Internet Safety courses at the beginning of any course or as part of the departmental induction. The guidance in this E-Safety Policy should be shared with staff, volunteers and participants by being accessible on the website and include a link to UK Safer Internet Centre.

https://www.saferinternet.org.uk/advice-centre/young-people

INCIDENTS AND RESPONSE

Where an e-safety incident is reported to the MK Dons Football Club this matter will be dealt with very seriously. MK Dons Football Club will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a participant wishes to report an incident, they can do so to their tutor/coach, a member of the Designated Safeguarding Team. Where a member of staff wishes to report an incident, they must contact their line manager or a member of the designated safeguarding team. Following any incident, the Designated Safeguarding Officer will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Whenever in doubt, employees and volunteers should contact the one of the designated safeguarding officers on the numbers below for advice and guidance.

Senior Safeguarding Manager -	John Cove	01908 622950
Designated Safeguarding Officer –	Jackie Bushell	01908 622950

SOCIAL MEDIA SAFETY

Conduct

Staff and volunteers are reminded that their professional responsibilities at MK Dons Football Club require them to act professionally in their social networking and internet activities, and to create a clear distinction between their **social** and their **professional** lives. Contact with participants must remain within the boundaries of their professional lives and contact with students should only be made through official MK Dons Football Club social media outlets. The guiding principle here is **"think before you post"**

(See MK Dons Football Club Safeguarding Policy and MK Dons Football Club Staff Handbook for further guidance on conduct)

Where staff make use of web-publishing and social networks for professional purposes they are expected to:

- Behave professionally and with integrity
- Adhere to Football Club policy guidelines
- Respect their audience
- Promote productive conversations
- Protect and enhance the value of the Football Club's reputation
- Protect confidential and business sensitive information
- Be personable, add value and encourage responses
- Be proactive in correcting any errors made

Staff and volunteers must not post comments or any other information on any public forum, website, social networking site or blog:

- That are unsubstantiated and/or negative about MK Dons Football Club (or other organisations within the Group), their colleagues, our participants, parents, or customers
- That run counter to MK Dons Football Club Equality and Diversity, and Safeguarding Policies.
- That recommend or appear to endorse law breaking of any kind
- That give an account of any inappropriate behaviour
- Nor should such comments be made in emails sent in an official or professional capacity.

Communications between staff and volunteers and current or prospective participants should only take place for legitimate, professional reasons. In some cases there may be a non- professional reason for a relationship to exist beyond the Football Club (e.g. common academic interest / common membership of a club, society or team / family members). In such circumstances social communication may occur. Staff should, however, be aware of the risks involved and use their professional judgment to ensure that this communication is limited appropriately.

A member of staff inviting a current or prospective participant to join a network without any professional purpose or inviting them to 'follow' a purely personal profile will be regarded as inappropriate and potentially subject to formal disciplinary action. The risks in this situation are clear and there can be no justification and it could be considered Gross Misconduct. Where such a situation arises MK Dons Football Club reserves the right to demand an explanation for this action and act accordingly.

Accepting any invitation to 'friend', follow or become part of a current or a prospective participants personal network is also considered inappropriate no matter what platform is used.

Do not create one to one communication channels via social media with participants that are U18 or are adults at risk.

We recognise staff may wish to take part in online communities also used by participants. In such cases staff should ensure that personal information is secured. Any staff member contributing under a personal profile is obliged to ensure that minimal personal information is visible under that profile.

OFFICIAL USAGE

As a general principle staff should use their MK Dons Football Club contact details or a 'professional' profile for communication with current and prospective participants, and ensure that any communication is both professional and necessary.

Email contact with participants, parents and other stakeholders should be channelled through the MK Dons Football Club email system. Staff should use the facility to Football Club up a forwarding email address where access to MK Dons Football Club webmail may present a problem.

Staff should pay particular attention when replying to emails forwarded to a personal account as these will appear to the recipient as having been sent from the personal account. MK Dons Football Club will continue to develop the use of social media for marketing, communications and education purposes.

To assist staff in posting factual and professionally presented information without using personal details line managers will coordinate guidance, support and training in the management of a professional online presence and appropriate and effective use of social networks as an educational and communication tool.

Authorised MK Dons Football Club networks (group/page/blog) which exist for a clear professional purpose should be discussed with the Senior Leadership Team who will offer advice and guidance on what is acceptable.

Staff creating or participating in authorised networks should do so either anonymously, where this is possible, or under a professional profile.

A **professional profile** is where a member of staff maintains an online presence explicitly for professional purposes. This profile should minimise any information which could be used to compromise the individual and should not be used to record social activity or personal opinion but may be used to record professional information or opinion. It is important that a professional profile is not added to non-professional networks or linked to the profiles of others except where the connection is professional. This might legitimately include links to participant groups but would be unlikely to include groups of friends / family.

MONITORING

Under certain circumstances the Football Club may need to monitor staff and participant email communication and use of the internet via the MK Dons Football Club internet link.

We recommend that staff monitor their own online presence, in particular, any material posted by others about them.

If staff become aware of, and / or are concerned about, any critical or unprofessional comments that are posted by colleagues they should draw these initially to the attention of the Designated Safeguarding Officer in order that an official response may be posted if appropriate.

It is the responsibility of line managers to monitor staff use of social networks in the workplace. In general, personal use is discouraged particularly where an alert service or other desktop 'widget' may interrupt workflow. Professional use should be transparent and any request to view interactions respected.

It is acknowledged that existing and new staff members may already have a significant online presence with membership of complex social-networks. It is the responsibility of staff to consider their existing and ongoing online activity in line with this policy guidance.

PARTICIPANT CONDUCT

As members of the MK Dons Football Club community, participants must abide by the terms of any learning agreement by respecting the rights of other participants and staff, as well as the reputation of MK Dons Football Club. They should think carefully about how they express themselves, and bear in mind the need to safeguard themselves.

Material posted on the internet can be hard to delete and should, therefore, be considered permanent.

Participants must not post comments on a social networking site or blog, or send text messages:

- That could be viewed as bullying or harassing another member of the Football Club community
- That are counter to MK Dons Football Club's Equality and Diversity policy
- That explicitly encourages other members of the community to break the law
- That are likely to bring MK Dons Football Club (or other organisations within the group) into disrepute
- Participants should not post photos that they might not wish others to see.
- Participants must not share photos that are deemed to be "youth produced sexual imagery".

Where staff become aware of this a procedure to follow is outlined in Annexe 1 of this policy. Participants should not invite staff to join social networks or follow purely personal profiles.

Participants will be given guidance on appropriate use of the internet and e-safety through tutorial and displays.

If a participant has cause for concern regarding use of the internet or social networking, they must report the incident immediately to a member of staff. There may be occasions where this will be treated as a safeguarding issue.

NOTES / DEFINITIONS

Open communication takes place in a public forum which can be viewed by unknown internet users i.e. the general public

Closed communication is where the participants are all known to each other. Most closed communication will be between two individuals (e.g. email exchange) but would also include 'friends only' groups or sites with registered members etc.

Public information is that which can be accessed anonymously by internet users who are unknown to the originator.

Private information is that which is only available to a limited, known sub-Football Club of internet users or solely by the owner of the information themselves.

The **originator** of online content is the individual who first uploads or creates the content using online tools.

Distribution - posting, uploading, adding, or forwarding digital content via electronic, web-based systems (including email) constitutes distribution of that content. A choice to publicly distribute private information is the responsibility of the distributor NOT the originator or the maintainer of the system used to distribute.
It is the responsibility of content originators to understand the system they are using and, where control cannot be guaranteed, to amend use of the system accordingly.

Adding content to online systems, other than those designed solely for storage purposes, will be seen as distribution of that content.

Content which is 'personal' in nature but made **available** to a public audience either deliberately or by carelessness will be considered the responsibility of the originator/ distributor of the content (e.g. the photographer NOT the subject of the photograph)

Whilst an initial interaction may be 'private', the content of any e-communication with a participant or parent must be considered permanent and de-facto public because there can be no guarantee sought or given that the student/parent will not re- distribute content publicly.

If private information is re-distributed without the consent of the originator this is the responsibility of the distributor. However, where such information is inappropriate it may be necessary for the originator to defend the initial process of distribution which placed it in a vulnerable position.

EQUALITY AND DIVERSITY

As with all MK Dons Football Club Policies and Procedures due care has been taken to ensure that this policy is appropriate to all employees regardless of gender, race, ethnicity, disability, sexual orientation, marital status, gender identity, religion or age.

The policy will be applied fairly and consistently whilst upholding MK Dons Football Club's commitment to providing equality to all.

ASSOCIATED GUIDANCE AND POLICIES

This policy is to be read and understood alongside the following guidance and policy documents that can be found on the shared drive or that can be provided to staff and volunteers on request:

· Safer Recruitment Policy

· Safeguarding Policy

· Dealing with allegations against employees/volunteers

· Female Genital Mutilation (FGM) Statement

· Prevent Strategy

· Child Sexual Exploitation Strategy

· Modern day Slavery Statement

USEFUL LINKS FOR FURTHER INFORMATION

Child Exploitation & Online Protection Centre: http://ceop.police.uk/

Child Exploitation & Online Protection: https://www.thinkuknow.co.uk/

Internet Watch Foundation: http://mobile.iwf.org.uk

DirectGov-'Staying Safe Online': http://www.nidirect.gov.uk/staying-safe-online

Get Safe Online: http://www.getsafeonline.org

http://www. childnet.com/ resources/picture-this

APPENDIX 1

GUIDANCE ON DEALING WITH YOUTH PRODUCED SEXUAL IMAGERY

The initial review meeting should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people.
- If a referral should be made to the police and/or children's social care.
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed.
- What further information is required to decide on the best response?
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment.
- If there is a need to contact another organisation, school, college, setting or individual.
- Whether to contact parents or carers of the people involved - in most cases parents should be involved.

An immediate referral to police and/or children's social care16 should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply then the Football Club may decide to respond to the incident without involving the police or children's social care (the Football Club can choose to escalate the incident at any time if further information/concerns come to light).

ASSESSING THE RISKS

The circumstances of incidents can vary widely. If at the initial review stage a decision has been made not to refer to police and/or children's social care, a further review (including an interview with the young people involved) should be made to establish the facts and assess the risks.

When assessing the risks the following should be considered:

- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?

- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities?
- Does the young person understand consent?
- Has the young person taken part in this kind of activity before?

CASE STUDY (SCHOOLS BASED)

Concern:

Two children, both aged 15, were in a relationship for the past month. The boy asked the girl for "sexy" pictures and she sent him a single topless photo. Afterwards the girl was worried that he might share the photo so she shared her concerns with her friends. Her friends then told their form tutor who spoke with the school DSL.

School response:

The tutor spoke with the girl and then the boy. Both pupils confirmed there had not been any sexual activity between them. There were not any wider safeguarding concerns about either pupil. There was no evidence that the image had been shared by the boy and he offered to delete the image from his device. Both pupils were spoken with by the designated safeguarding officer/PCSO who advised them on the potential impact of taking and sharing youth produced sexual imagery both criminally and emotionally. The designated safeguarding officer documented the incident and as well as the actions taken in the children's safeguarding records.

Young people may need help and support with the removal of content (imagery and videos) from devices and social media, especially if they are distressed. Most online service providers offer a reporting function for account holders and some offer a public reporting function to enable a third party to make a report on behalf of the young person.