



## Leicester City School Sport & Physical Activity Network Social Media Policy

**Associated Policies:** **Child Protection and Safeguarding Policy**  
**GDPR Policies and Guidance**  
**Health and Safety Policy**  
**Code of Conduct for host schools/academies**

Version	Created	Review Date
1.3	October 2020	October 2021

### Introduction

Leicester City School Sport & Physical Activity Network recognises and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

### 1. Aims of this policy

- 1.1. Leicester City School Sport & Physical Activity Network (LCSSPAN) aims to:
  - encourage good practice in the use of social media by staff, partners and followers.
  - protect LCSSPAN and its employees by minimising the risks of inappropriate use of social media by staff, students and visitors.
  - ensure that social media is used safely and responsibly as an effective part of LCSSPAN activities and promotion.
  - ensure that all issues arising from inappropriate use of social media are dealt with quickly effectively and within policy guidelines.
- 1.2. This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Instagram, Whatsapp, TikTok, Snapchat and all other social networking sites, internet postings, blogs and chat apps.
- 1.3. The policy applies regardless of whether the social media platform is accessed using the school's IT facilities and equipment, or devices belonging to members of staff.

## **2. Roles, responsibility and procedure**

### 2.1. Employees should:

- be aware of their online reputation, and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media.
- ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer.
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, other employees of the trust, or even future employers, to read. If in doubt, don't post it!

### 2.2. Managers are responsible for:

- addressing any concerns and/or questions employees may have on the use of social media.
- operating within the boundaries of this policy, and ensuring that all staff understand the standards of behaviour expected of them.

### 2.3. Host Schools (Employers) are responsible for:

- giving specialist advice on the use of social media.
- implementing and reviewing this policy.

## **3. Scope of this policy**

### 3.1. The policy:

- applies to all employees, officers, consultants, contractors, volunteers, visitors, casual workers and agency workers within LCSSPAN.
- applies to the use of social media for business purposes as well as personal use that may affect the organisation or its partner schools in any way.
- ensures LCSSPAN's commitment to safeguard children, the reputation of the host schools and those who work for it and the wider community.
- does not form part of any employee's contract of employment and may be amended at any time.

## **4. Purpose of this policy**

- 4.1. Our purpose is to ensure safe internet and social media use by staff, students and visitors as an essential part of our safeguarding duty of care for all.

## **5. Who is responsible for carrying out this policy?**

5.1. The implementation of this policy will ultimately be monitored by the Local Governing Body of each SSPAN host school/academy. However, the delegated day-to-day responsibility for its operation falls to the LCSSPAN School Sport Development Managers (SSDM).

5.2. Line Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

5.3. All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the SSDM's,

or to the host schools DSL. Questions regarding the content or application of this policy should be directed to the SSDM's, or to the host schools DSL.

## **6. Legislation and statutory guidance**

- 6.1. LCSSPAN is committed to ensuring that all staff provide confidential services that meet the highest standards.
- 6.2. All individuals working on behalf of LCSSPAN, through their employment by host schools/academies, are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:
  - The Human Rights Act 1998
  - Common law duty of confidentiality, and
  - The Data Protection Act 1998
- 6.3. Confidential information includes, but is not limited to:
  - Person-identifiable information, e.g. young people and employee records protected by the Data Protection Act 1998
  - Information divulged in the expectation of confidentiality
  - Academy business or corporate records containing organisationally or publicly sensitive information
  - Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
  - Politically sensitive information
- 6.4. LCSSPAN Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:
  - Libel Act 1843
  - Defamation Acts 1952,1996 and 2013
  - Protection from Harassment Act 1997
  - Criminal Justice and Public Order Act 1994
  - Malicious Communications Act 1988
  - Communications Act 2003, and
  - Copyright, Designs and Patents Acts 1988

## **7. Safeguarding**

- 7.1. The use of social networking sites introduces a range of potential safeguarding risks to children and young people. Potential risks can include, but are not limited to:
  - online bullying
  - grooming, exploitation or stalking
  - exposure to inappropriate material or hateful language
  - encouraging violent behaviour, self-harm or risk taking
- 7.2. In order to mitigate these risks, there are steps you can take to promote safety online:

- you should not use any information in an attempt to locate or meet a child. the online activity of students and other colleagues, and
  - ensure that any messages, photos or information comply with existing policies.
- 7.3. This includes their duties relating to Children Missing Education, Child Sexual Exploitation, FGM and Preventing Radicalisation (Prevent).

## **8. Reporting Safeguarding Concerns**

- 8.1. Any content or online activity which raises a safeguarding concern must be reported to the lead safeguarding officer in the school/trust. Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child. With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

## **9. Reporting, responding and recording cyberbullying incidents**

- 9.1. Staff should never engage with cyberbullying incidents. If in the course of your employment with this school/trust, you discover a website containing inaccurate, inappropriate or inflammatory written material relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a senior manager at your school.
- 9.2. Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

## **10. Overview**

- 10.1. Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to breach any of the following host school/academy policies and agreements:
- Online Safety Policy (e-Safety)
  - Acceptable Use Policy
  - Disciplinary Policy
  - Anti-Bullying and Harassment Policy
  - Equal Opportunities Policy
  - Data Protection Policy (for example, never disclose personal information about a colleague or student online)
  - GDPR Policies and Guidance
  - Any other laws or regulatory requirements
- 10.2. LCSSPAN Staff who breach any of the above policies will be subject to disciplinary action by their host school/academy employer, and possibly termination of employment.
- 10.3. Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of reference and the organisation.
- 10.4. Staff must make themselves aware of and act in accordance with their duties under the DfE statutory guidance Keeping Children Safe in Education 2019 as this relates to:

- their own online activity;
- the online activity of students and other colleagues, and
- information of which they become aware of online.

10.5. This includes their duties relating to Children Missing Education, Child Sexual Exploitation, FGM and Preventing Radicalisation (Prevent).

## **11. Personal Use of Social Media**

11.1. Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

11.2. Personal use of social media at 'off duty' times during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or working practice and complies with this policy.

11.3. You should:

- avoid making any social media communications that could damage the organisation or that of the host school/academy's interests or reputation, even indirectly.
- not use social media to defame or disparage the organisation, host school/academy, our staff, students, parents/carers or any third party; to harass, bully or unlawfully discriminate against students, parents/carers, staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.
- not express opinions on our behalf via social media, unless expressly authorised to do so by your line manager. You may be required to undergo training in order to obtain such authorisation.
- not post comments about sensitive, confidential information, organisation or host school/academy related topics.
- not accept students or their parent/carers as friends or use social media to send any personal messages to them directly or indirectly – personal communication could be considered inappropriate and unprofessional and may put you and/or your colleagues vulnerable to allegations.
- not share any personal information with any student (including personal contact details, personal website addresses/social networking site details) and ensure good safeguarding practice.

11.4. You are strongly advised not to be friends (on or off line) with recent students (the potential for colleagues within the organisation or host school/academy to be compromised in terms of content and open to accusations makes the risk not worth taking). You are also strongly advised not to be friends with students at other schools (on or offline) as this is likely to make them vulnerable to allegations and may be open to investigation by the organisation, host school/academy or the police. Where a colleague is considering not following this advice, they are required to discuss the matter, and the implications, with the host school/academy Principal or Designated Safeguarding Lead.

11.5. Caution is advised when inviting work colleagues to be 'friends' on personal networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationship; it could be embarrassing if too much personal information is known in the work place.

- 11.6. You must not post or share photographs of students under any circumstances.
- 11.7. Any misuse of social media should be reported to the host school/academy Designated Safeguarding Lead and the host school/academy Principal.

## **12. Guidelines for responsible personal use of social media**

- 12.1. You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.
- 12.2. You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the organisation or host school/academy and your personal interests.
- 12.3. Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.
- 12.4. If you disclose your affiliation with the organisation or host school/academy on your profile or in any social media postings, you must state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present at work, to the community and colleagues.
- 12.5. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager. All communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended (social networking sites are public forums). You are strongly advised, in your own interests, to take steps to ensure as far as possible that their on-line personal data is not accessible to anybody who they do not want to have permission to access it. For example, you are strongly advised to check the security and privacy settings of any social networking site you subscribe to and set these to maximum and, where relevant, use strong passwords and change them regularly. For further information, see the safer internet website <http://www.saferinternet.org.uk/> and the South West Grid for Learning Resources <http://www.swgfl.org.uk/Staying-Safe>
- 12.6. For further information about the safe, secure and proper use of social media and networking sites, please see <http://www.childnet.com/resources/socialnetworking-a-guide-for-teachers-and-professionals>
- 12.7. If you see social media content that disparages or reflects poorly on the organisation or host school/academy you should contact your manager and the host school/academy Principal.

## **13. Educational Use of Social Media**

- 13.1. When using social media for educational purposes, the following practices should be observed:
  - Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to a LCSSPAN email account;
  - The content of any organisation or host school/academy-sanctioned social media site should be solely professional and should reflect well on the organisation or host school/academy;
  - Staff must ensure that the organisation has parent/carer consent to use, post or publish a photograph or video image of the student. Please see paragraph below in respect of parent/carer consent;

- Staff must ensure that they do not identify a student using their full name. Only first/forenames or initials may be used;
- Care must be taken that any links to external sites from the account are appropriate and safe;
- Any inappropriate comments on or abuse of organisation or host school/academy - sanctioned social media should immediately be removed and reported to the host school/academy DSL or IT Director;
- Staff should not engage with any direct messaging of students through social media where the message is not public;
- Staff should not seek to view/link up with view student accounts. For example, in the case of Twitter, staff should not “follow back” those who follow, share or like organisation or host school/academy comments/posts.

13.2. The failure to follow the rules set out may give rise to disciplinary action.

13.3. The use of social media for business purposes is subject to the remainder of this policy.

## **14. Parent/carer consent**

- 14.1. At each LCSSPAN event or session attending schools should be asked to identify any young people who have not got consent from their parent/guardian to have photos or videos taken of them and used for organisation related purposes.
- 14.2. Children for which the schools do not have consent for photography should be clearly identified in a positive way, and all staff/volunteers & spectators should be made aware of this in the pre-event briefing.
- 14.3. Organisation staff should familiarise themselves with these students throughout the course of the event/session, and question individuals who may be taking photos or videos of them. It is a disciplinary offence to use, post or publish a photograph or video image of a student contrary to the instructions of their parent/carer.

## **15. Monitoring**

- 15.1. We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.
- 15.2. We reserve the right to contact the Professionals Online Safety Helpline to assist with monitoring.

## **16. Action by employer – inappropriate use of social media**

- 16.1. Following a report of inappropriate use of social media, the senior manager will conduct a prompt investigation.
- 16.2. If in the course of the investigation, it is found that a pupil submitted the material to the website, that pupil will be disciplined in line with the school’s behaviour policy.
- 16.3. The senior manager, where appropriate, will approach the website hosts to ensure the material is either amended or removed as a matter of urgency, ie within 24 hours. If the website requires the individual who is complaining to do so personally, the school will give their full support and assistance.

- 16.4. Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website.
- 16.5. If the material is threatening and/or intimidating, senior management will, with the member of staff's consent, report the matter to the police.
- 16.6. The member of staff will be offered full support and appropriate stress counselling.

## **17. Breach of this policy**

- 17.1. Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff 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.
- 17.2. You may be required to remove any social media content that we consider to be a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

## **18. Impact on Working Hours and Work – Life Balance**

- 18.1. The implementation of this policy should have minimal impact on workload and work life balance. However, if the reporting and recording which is necessarily associated with this policy proves to be very onerous and begins to have an impact on workload, this will be taken account of in a review.

## **19. Monitoring and Review of this Policy**

- 19.1. If the manager reasonably believes that an employee has breached this policy, from time to time the school will monitor or record communications that are sent or received from within the school/trust's network.
- 19.2. The SSDM in partnership with the host school/academy has overall responsibility for the adoption, review and amendments of this policy. The policy will be reviewed annually, or earlier if necessary, to comply with statutory DfE updates and amendments.