



**Personal Use of Social Media Sites**

This policy has been provided by Leicestershire County Council Traded Services following consultation with unions. It has been adopted in its entirety by the Governing Body of King Edward VII Science and Sport College.

It is reviewed regularly and was last reviewed in January 2016.

Signed ..... J.T. Kailofer

## Scope

This policy applies to support staff, Teachers and Headteachers / Principals (*and within this policy will be referenced as employee(s) or academy staff*), based in Schools, Colleges or Academies (*and within this policy will simply be referenced as Academy(s)*).

This policy also applies to Academy Governors as detailed below.

## Application of this Policy to Academy Governors

Whilst some aspects of this Policy are clearly more targeted at academy staff, many have equal application to governors. For example, the Policy provides guidance for all on what is considered to be inappropriate use of social media/internet sites. All governors should ensure that they comply with the spirit of the policy.

Though governors would not be subject to the same disciplinary process as staff, there are still forms of redress available where a governor behaves in an inappropriate manner. The appropriate procedures would be followed in such cases.

## Purpose

This policy serves two main purposes. Firstly, it is to support the safe, effective use of social media in an education setting, and, secondly it is to clarify how employees should conduct themselves when using all forms of social networking websites and blogs, in one's own time.

Employees wanting to have a work-related social media presence must discuss this with and obtain the relevant approval from, the Principal.

If followed, it will guide employees on how to minimise the risk they may place themselves and students in, when they choose to write about their work or matters relating to the academy and their personal lives. This in turn will minimise situations where safeguarding concerns could arise, employees' integrity or professional standing could be undermined, or the Academy and / or the Local Authority brought into disrepute and professional relationships with colleagues and students compromised.

Additionally, adhering to the policy reduces the risk of employees inadvertently contravening sections of the Data Protection Act or falling foul of any breaches of confidentiality, privacy, libel, defamation, harassment and copyright laws.

This policy is not intended to prevent employees from using social media sites, but to make them aware of the risks they could face, when sharing information about their professional and/or personal life. Employees should be encouraged to report any concerns that they have regarding content placed by employees on social media sites to the Principal.

## Social Media Definition

Social media can be defined as websites and applications that enable users to create and share content or to participate in social networking, resulting in a number of different activities.

These activities can include, but are not limited to:

- Maintaining a profile page on social / business networking sites such as Facebook, Twitter or LinkedIn
- Writing or commenting on a blog, whether it is your own or the blog of another person / informational site
- Taking part in discussions on web forums or message boards
- Leaving product or service reviews on business websites or customer review websites
- Taking part in online polls
- Uploading multimedia on networking sites such as Instagram and Tumblr
- Liking, re-tweeting and commenting on posts of your own, another person or other social media account

## Professional Use of Social Media

Where staff wish to use social media for professional use they should create a separate online presence that is entirely segregated from their personal online presence. Although standards as set out in this document should be upheld within both presences, this separation will reduce the risk of inadvertent networks being created with students.

eg.

- Separate Twitter accounts that do not follow each other. For academy owned accounts access should be shared with the principal.
- Professional Google accounts to allow use of google drive/blogger without connecting with home internet use.

Other guidance:

- Do not “Follow Back” students on Twitter - this removes the potential for Direct Messaging
- Remember that Twitter is an open network and should be treated as such.
- Facebook is unlikely to support a safe, segregated network for professional use
- Blogs can be used to easily share resources without the need to make individual connections but again should be seen as extensions of the academy website and should be moderated accordingly.

NOTE:

The academy recognises 3 types of social media presences:

- Personal – for own use, including teacher networking
- Academy endorsed – professional use, for sharing resources with students
- Academy owned – professional use, access is shared with the academy

All staff should be aware of which type they have and act accordingly. Intellectual property within such sites is in line with individual contracts.

In all circumstances it is recommended that advice is sought from appropriate people BEFORE creating/using social media in academy and relevant approval MUST be sought as defined above.

## Personal Use of Social Media

As with all personal internet use, employees using social media sites must observe the specific requirements of the Academy's E-Safety Policy.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against employees and the Academy. It may also cause embarrassment to the Academy and other parties connected to the Academy or bring such parties into disrepute.

Any such action would likely be addressed under the Disciplinary Policy and could result in summary dismissal.

Where evidence of misuse is found, a more detailed investigation in accordance with the Disciplinary Policy may be necessary, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary such information may be handed to the police.

If you become aware of any use of social media by other members of staff in breach of this policy then the matter should be reported to the Principal.

## Employee Responsibility

- Employees are personally responsible for the content they publish on social media sites, including likes/re-tweets etc. Employees should assume that everything that is written is permanent and can be viewed by anyone at any time.
- Employees should assume that everything can be traced back to them personally as well as to their colleagues, the Academy and parents.
- To avoid any conflict of interest, employees should ensure that personal social networking sites are set at private and students are never listed as approved contacts. An exception to this may be if the child is the employee's own child, or relative.
- Information must not be posted that would disclose the identity of students.
- Employees must ensure content or links to other content does not interfere with their work commitments
- Students must not be discussed on social media sites.
- Photographs or videos of students or their homes must not be posted on social media sites.
- Employees should not post information on sites, e.g. photographs and videos that could bring the Academy or the Local Authority into disrepute.
- Employees must not represent their own views/opinions as being those of the Academy or the Local Authority.

- Potentially false or defamatory remarks towards the Academy, the Local Authority, employees, students, students' relatives, Academy or Local Authority suppliers and partner organisations should not be posted on social media sites.
- Employees must not either endorse or criticise service providers used by the Academy or the Local Authority or develop on-line relationships which create a conflict of interest.
- When posting on social media sites employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive, obscene, derogatory, discriminatory language which may cause embarrassment to Academy, the Local Authority, employees, students, students' relatives, Council suppliers and partner organisations.
- Employees must not divulge any information that is confidential to the Academy, the Local Authority or a partner organisation.
- Employees must not upload, post, forward or post a link to any pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- Employees must not upload, post, forward or post a link with regards to any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

This list is not exhaustive.

## Disciplinary Action

Employees should be aware that the use of social media sites in a manner contrary to this policy, including if others implicate you in a breach of any of the terms listed above may result in disciplinary action and in serious cases may be treated as gross misconduct, which itself could lead to summary dismissal.

Any instances of “cyber bullying” will initially be addressed under the Dignity at Work Policy and Procedure and may result in disciplinary action.

## Social Media Security

Employees should be mindful when placing information on social media sites that this information is visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for false allegations and threats. In addition it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security.

Furthermore there is the scope for causing offence or unintentionally causing embarrassment, for example if students find photographs of their teacher which may cause embarrassment and/or damage to their professional reputation and that of the Academy. In addition, it may be possible for other social media site users to identify where employees live, which could have implications for individual security.

Therefore, first and foremost consideration should be given to the information posted on social media sites and employees are advised to use appropriately the security settings on such sites in order to assist in limiting the concerns above.

## **Monitoring the use of Social Media Websites**

Employees should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under the Disciplinary Policy.

The Academy considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been using social media websites when he/she should be working; or
- acted in a way that is in breach of the rules set out in this policy.

## **Employee Groups / Networks**

Employee groups can be created on social media sites such as Facebook. Creators of these groups are responsible for monitoring the content of the site and ensuring that it is appropriate and not in breach of any of the terms in this policy.