Social Media Policy

This policy provides guidance on what measures are to be taken to ensure the safe use of social media and defines what is considered to be inappropriate conduct when using social media/internet sites for both professional and personal purposes.

Version number	V3.0
Consultation groups	Headteachers, Central services and JCC
Approved by	Trust Leader
Approval date	9th March 2022
Adopted by	All Schools
Adopted date	9th March 2022
Policy/document owner	Director of IT/ Director of Operations
Status	Approved – final
Frequency of review	Every three Years
Next review date	January 2025
Applicable to	All Employees

This policy has been written with consideration given to working practices. By adopting this policy, a reduction in workload has been facilitated by reducing the need for individual academies to interpret the policy locally

Document History

Version	Version Date	Author	Summary of Changes
V0.1	15.5.18	Louise Barber - Director of Operations	New policy prepared using Leicestershire County Council Version: 2016 – MA1 v2, Agreed at: JCC 8th February 2017
V1.0	29.4.19	Helen Stockill – Head of Governance	Updated references to the governance structure, added in information on affiliate links on personal social media sites. Included a responsibility in relation to expressing political opinions and social media relationships with parents.
V2.0	6.5.19	Paul Stone – CEO	Reviewed and agreed.
V2.1	28.5.19	Louise Barber - Director of Operations	Expanded point 8.3 to include social media expectations in family groups
V2.2	9/02/2022	Louise Barber - Director of Operations	Reviewed in line with review period - minor edits made to reflect role name changes only.
V2.2	9/03/2022	Louise Barber - Director of Operations	JCC approved with minor edits to 8.2 – 'No Exceptions'
V3.0	9/03/2022	Louise Barber - Director of Operations	Trust Leader approved

Contents

1. Scope

This policy applies to all Discovery Schools Academy Trust staff, regardless of whether they are permanent, fixed term, casual or agency or volunteers (and within this policy will be referenced as employee(s) or DSAT staff), based in all schools and corporate offices, (and within this policy will simply be referenced to as School(s)).

This policy also applies to Trustees, Governors and Advisory Board Members as detailed in section 2.

The policy applies to all use and all forms of social media where there is potential impact on the school or Trust, whether for work-related or personal use, during working hours or otherwise. Breaches of this policy may be dealt with via the Trust's disciplinary policy or where it is appropriate will be referred to the police.

2. Application of this policy to Trustees, Governors and Advisory Board Members

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

Though Trustees, Governors and Advisory Board Members would not be subject to the same disciplinary process as staff, there are still forms of redress available through the Governance Code of Conduct agreement. The appropriate procedures would be followed in such cases.

3. Documents to support this policy:

In addition, this policy should also be read in conjunction with:

- The trust/ school handbooks
- Code of Conduct
- ICT acceptable Use Policy
- Online Safety Policy

Flick Training should also be completed.

4. Purpose

The primary purpose of this policy is to clarify how all employees should conduct themselves when using all forms of social media whether this is done through the school's media or personal media, in work time or in an individual's own time. The aim being to minimise the risk employees may place themselves and pupils in when they choose to write about their work or matters relating to the school and/or their personal lives.

This in turn will minimise situations where safeguarding concerns could arise, employees' integrity or professional standing could be undermined, professional relationships with colleagues and pupils are compromised or the school brought into disrepute.

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

Whilst this policy is not intended to prevent employees from using social media sites, it does aim to make employees aware of the risks they could face whilst doing so and highlight what is deemed to be unacceptable 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 Headteacher.

When an employee(s) wishes to create a work-related social media site they must discuss this with and obtain the relevant approval from the Headteacher. 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.

5. Application of the Policy

The policy will be managed by either the Headteacher or another manager with support of the HR Manager. If the matters are regarding the Headteacher, then the Director of Education/ Deputy Trust Leader (SEN) will be responsible for overseeing this policy with support of the HR Manager. If the matters are regarding members of the Central Service team, then the HR Manager will be responsible for overseeing this policy.

Commented [LB1]: Replaced Executive Team with HR Manager

Commented [LB2]: Refreshed this section to ensure role names were current

6. Definition of Social Media

For the purposes of this policy, the term social media is used to describe a type of interactive website or online tool that allows parties to communicate or interact with each other in some way by sharing information, opinions, knowledge and interests and to share data in a public forum or to participate in social networking, resulting in a number of different activities.

Social Media activities include, but are not limited to:

- Maintaining a profile page on social / business networking sites such as Facebook, Twitter, WhatsApp 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 such as YouTube
- Leaving product or service reviews on business websites or customer review websites
- Taking part in online polls
- Uploading multimedia on networking sites such as You Tube, Instagram, WhatsApp, Twitter and Tumblr
- Liking, re-tweeting and commenting on posts of your own, another person or other social media account

Many other forms of social media also exist which are not listed in this policy. Employees need to be aware that this is area is constantly changing and they are reminded of their continued responsibility to keep up to date with developments and review their privacy settings on a regular basis when using social media sites.

7. The Use Of Social Media

The Trust recognises that employees will use social media in a personal capacity. However, it is important that employees understand that they are personally responsible for all comments, images or information that they post online. Therefore, all employees must ensure that when posting any information, images or making comments, they do not:

- **Bring the School or Trust into disrepute**. E.g. by making political, derogatory or defamatory comments, either directly or indirectly, about the school, colleagues, individuals, pupils or parents etc that could negatively impact on the school's reputation or cause embarrassment. This includes posting images or links to inappropriate content or using inappropriate language.

- **Breach confidentiality**. E.g, revealing confidential information owned by the school relating to its activities, finances, employees or pupils.

- **Undertake any behaviour which may be considered discriminatory, or as bullying and/or harassment of any individual**. E.g, making offensive or derogatory comments (either directly or indirectly) relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully

("Cyberbullying") another individual; or posting images that are discriminatory or offensive or linking to such content.

When personally engaging on social media, a school/trust affiliation on an employee's profile has the ability to affect the Trust as a whole. Employees should be aware of the risk this presents and that it carries with the responsibilities which have been set out in this policy.

As with all personal internet use, employees using social media sites must also observe the specific requirements of the documents named at the beginning of this policy.
School social media accounts should be treated as professional channels.

8. Employee responsibilities

Employees are personally responsible for the content that they publish on social media sites, including but not limited to; "Likes" (on Facebook)/"re-tweets" (on Twitter), Snapchat, Instagram, LinkedIn, Yammer, WhatsApp etc.

Employees should assume that everything that is written is permanent and can be viewed by anyone at any time. It is fair and reasonable to take disciplinary action against employees for inappropriate use of social media, including use of social media conducted outside of working hours.

Employees must observe and note the following listed guidance (which is not exhaustive).

8.1. Employees should assume that everything can be traced back to them personally as well as to their colleagues, the school, pupils and parents.

8.2. To avoid any conflict of interest, employees must ensure that personal social networking sites are set to private and pupils are never listed as approved contacts. There may be exceptions where a pupil is a family member or close personal family relationship.

8.3. In order to maintain professional boundaries, staff should not accept or initiate personal invitations to be friends on social media or "followed" on social media from parents of the school unless they know them in a personal capacity (such as being family members themselves) prior to their appointment and/or have specific permission to do so by the Senior Designated Lead for the school.

8.4. Information must not be posted that would disclose the identity of pupils or could in any way be linked to a pupil(s). This includes photographs or videos of pupils or their homes

8.5. Pupils must never be discussed on social media sites.

8.6. Employees should not post information on sites including photographs and videos that could bring the School into disrepute.

8.7. When posting on social media sites employees must observe the requirements of data protection regulations.

8.8. Employees must not represent their own views/opinions as being those of the school or trust.

8.9. Employees must not divulge any information that is confidential to the school, trust or a partner organisation.

8.10. Potentially false, derogatory, offensive or defamatory remarks directly or indirectly towards the School, employees, pupils, pupils' relatives, the school suppliers and partner organisations should not be posted on social media sites.

8.11. Employees must avoid the appearance (including affiliation to the Trust on personal social media sites) that they are speaking or acting for the School/Trust when engaging in political activities. Expressing political opinions and engaging in political activities can be done in an individual capacity only.

8.12. Employees must ensure content or links to other content does not interfere with their work commitments or be on an inappropriate content.

8.13. Employees must not either endorse or criticise service providers used by the school or develop on-line relationships which create a conflict of interest.

8.14. 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).

8.15. 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 also cause embarrassment to school, employees, pupils, pupils' relatives, school suppliers and partner organisations.

8.16. Employees must never impersonate another person.

8.17. Employees must not upload~~,~~ forward or post a link which is likely to: create any liability for the School (whether criminal or civil), breach copyright law or other affect intellectual property rights, or which invades the privacy of any person.

THINK BEFORE YOU POST. There is no such thing as a private social media site. Social networking platforms/ Chat Rooms and discussion forums etc are in the public domain and it is not always possible to be sure what is being viewed, shared or archived, even if material is posted on a closed profile or group. There can be no reasonable expectation that posts will remain private and will not be passed on to other people, intentionally or otherwise.

9. 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 points listed within this document* may result in disciplinary action and in serious cases may be treated as gross misconduct, which itself could lead to summary dismissal.

In certain circumstances, such misuse may constitute a criminal offence or otherwise give rise to legal liability against employees and the school. Such cases will be referred to the police (and, where necessary the nominated safeguarding lead at the County Council) to investigate further.

Employees who become aware of any use of social media by other members of staff in breach of this policy must report the matter to the Headteacher or relevant manager.

10. 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 identify fraud, 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 and be in breach of data protection regulations. Employees should therefore be mindful that they:

- Do not reveal personal or private information about themselves such as date of birth, address details and bank details etc. Posting such information could increase the risk of identity theft.
- Remember that there is the scope for causing offence or unintentionally causing embarrassment, for example if pupils find photographs of their teacher which may cause embarrassment and/or damage to professional reputation and that of the School.
- Be mindful that posting images, comments or joining on line campaigns may be viewed by colleagues, parents, ex-pupils etc.
- Ensure that where you do post comments make a clear statement that any comments expressed are your own and not those of the school/trust

Finally, 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.

11. 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 trust 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.

12. 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. Please refer to the Director of IT for further guidance about such groups.