



BEIS YAAKOV JEWISH HIGH SCHOOL ACADEMY

SOCIAL MEDIA POLICY

Date of approval	August 2021
Date of next review	August 2024
Term of review	3 years
Committee Responsible	
Prepared By	Rabbi N Wilson
Signed and dated by Chair of Committee	

Changes Made	Date

Contents

1.	Policy statement	3
2.	Who is covered by the policy?	3
3.	Scope and purpose of the policy	3
4.	Personnel responsible for implementing the policy	4
5.	Compliance with related policies and agreements	4
6.	Personal use of social media.....	5
7.	Monitoring and data protection	5
8.	Business use of social media	6
9.	Recruitment	6
10.	Responsible use of social media.....	6
11.	Review of policy	8

1. Policy statement

- 1.1 We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to our ability to safeguard children and young people, protect confidential information and reputation, and can jeopardise our compliance with legal obligations. This could also be the case during off duty time.
- 1.2 Employees using social media are also potentially at risk of others misunderstanding the intent behind online communications or blurring of professional boundaries between children and young people and their parents or carers. This policy therefore sets out the academy's expectations regarding the use of social media.
- 1.3 To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes, and that the use of personal devices does not have an adversary impact on our business we expect employees to adhere to this policy.
- 1.4 This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. Who is covered by the policy?

- 2.1 This policy covers all employees working at all levels and grades. It also applies to consultants, contractors, casual and agency staff and volunteers (collectively referred to as **staff** in this policy).
- 2.2 Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

3. Scope and purpose of the policy

- 3.1 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, WhatsApp, all other social networking sites, and all other internet postings, including blogs.
- 3.2 It applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.
- 3.3 Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. 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.

- 3.4 Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

4. Personnel responsible for implementing the policy

- 4.1 The Governing Board has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Executive Principal. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Executive Principal.
- 4.2 All 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. [Managers will be given training in order to do this.]
- 4.3 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 Executive Principal. Questions regarding the content or application of this policy should be directed to the Executive Principal.

5. Compliance with related policies and agreements

- 5.1 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, employees are prohibited from using social media to:
- (a) Breach our ICT user policy;
 - (b) Breach our obligations with respect to the rules of relevant regulatory bodies;
 - (c) Breach any obligations they may have relating to confidentiality;
 - (d) Breach our Disciplinary Rules;
 - (e) Defame or disparage the academy or its affiliates, governors, students, parents and carers, staff, business partners, suppliers, vendors or other stakeholders;
 - (f) harass or bully other staff in any way or breach our Anti-harassment and bullying policy;
 - (g) unlawfully discriminate against other staff or third parties or breach our Equal opportunities policy;
 - (h) Breach our Data Protection Policy (for example, never disclose personal information about a colleague online);
 - (i) Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

- 5.2 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 Academy and create legal liability for both the author of the reference and the Academy.
- 5.3 Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

6. Personal use of social media

We recognise that employees may work long hours and occasionally may desire to use social media for personal activities at work or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the Academy's business are also prohibited.

7. Monitoring and data protection

- 7.1 The contents of our IT resources and communications systems, held in whatever media, including information and data held on computer systems, hand-held devices, tablets or other portable or electronic devices and telephones, relating both to the Employer's own education provision or any pupils, clients, suppliers and other third parties with whom the Employer engages or provides educational provision for, remains our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.
- 7.2 We may monitor intercept and review, without further notice, employee 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 are for legitimate business purposes. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.
- 1.1 We will comply with the requirements of **Data Protection Legislation** (being (i) the General Data Protection Regulation ((EU) 2016/679) (unless and until the GDPR is no longer directly applicable in the UK) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998, including the Data Protection Act 2018), in the monitoring of our IT resources and communication systems Monitoring undertaken is in line with our Workforce Privacy Notice which sets out how we will gather, process and hold personal data of individuals during

their employment. Our Data Protection Policy sets out how we will comply with Data Protection Legislation.

- 7.3 In line with the requirements of Data Protection Legislation, we may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice. Records will be kept in accordance with our Retention and Destruction Policy.
- 7.4 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the Academy.
- 7.5 For further information, please refer to our ICT user policy and Data Protection Policy.

8. Business use of social media

- 8.1 If your duties require you to speak on behalf of the Academy in a social media environment, you must still seek approval for such communication from your manager, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.
- 8.2 Likewise, if you are contacted for comments about the Academy for publication anywhere, including in any social media outlet, direct the inquiry to the Executive Principal and do not respond without written approval.
- 8.3 The use of social media for business purposes is subject to the remainder of this policy.

9. Recruitment

- 9.1 Unless it is in relation to finding candidates (for example, if an individual has put his/her details on social media websites for the purpose of attracting prospective employers), the Academy will not, either themselves or through a third party, conduct searches on applicants on social media. This is because conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with the Academy's Equal opportunities policy.

10. Responsible use of social media

- 10.1 The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely and in order to protect staff and the academy.
- 10.2 Employees' use of social media can pose risks to our ability to safeguard children and young people, protect our confidential information and reputation, and can jeopardise our compliance with our legal obligations. This could also be the case during off duty time.
- 10.3 Safeguarding children and young people:

- (a) You should not communicate with pupils over social network sites. You must block unwanted communications from pupils.
- (b) You should never knowingly communicate with pupils in these forums or via personal email account or using your school e-mail account where the communication is non-school related.
- (c) You should not interact with any ex-pupil of the Academy who is under 18 on such sites.
- (d) Communication with pupils should only be conducted through our usual channels. This communication should only ever be related to our business.

10.4 Protecting our business reputation:

- (a) Staff must not post disparaging or defamatory statements about:
 - (i) our Academy;
 - (ii) our students or their parents or carers;
 - (iii) our governors or staff;
 - (iv) the local community/communities of which the parent body are a part
 - (v) suppliers and vendors; and
 - (vi) other affiliates and stakeholders,

but staff should also avoid social media communications that might be misconstrued in a way that could damage our Academy reputation, even indirectly.

- (b) Staff should make it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal e-mail address when communicating via social media.
- (c) Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses including the Academy itself, future employers and social acquaintances, for a long time. Keep this in mind before you post content.
- (d) If you disclose your affiliation as an employee of our Academy, you must also state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not represent the views of my employer". You should also ensure that your profile and any content you post are consistent with the professional image you present to students and colleagues.
- (e) Avoid posting comments about sensitive Academy-related topics, such as our performance. Even if you make it clear that your views

on such topics do not represent those of the Academy, your comments could still damage our reputation.

- (f) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with the Executive Principal.
- (g) If you see content in social media that disparages or reflects poorly on our Academy or our stakeholders, you should print out the content and contact Executive Principal. All staff are responsible for protecting our Academy's reputation.

10.5 Respecting intellectual property and confidential information:

- (a) Staff should not do anything to jeopardise our confidential information and intellectual property through the use of social media.
- (b) In addition, staff should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the Academy, as well as the individual author.
- (c) Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.
- (d) To protect yourself and the Academy against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Executive Principal.
- (e) The contact details of business contacts made during the course of your employment are regarded as our confidential information, and as such you will be required to delete all such details from your personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

10.6 Respecting colleagues, students, parents and carers, governors and other stakeholders:

- (a) Do not post anything that your colleagues or our students, parents and carers, governors and other stakeholders would find offensive, including discriminatory comments, insults or obscenity.
- (b) Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission.

11. Review of policy

- 11.1 This policy is reviewed every 3 years by the Executive Principal. We will monitor the application and outcomes of this policy to ensure it is working effectively.