



Social Networking Policy for Academy based employees

Adopted By: Sunnyside Academy

Date: July 2020

1.0 Introduction

- 1.1 This policy is to ensure that all employees are aware of their responsibilities in connection with the use of social networking sites. It recognises that the use of such sites have become a significant part of life for many people and provide a way of keeping in touch with friends and colleagues, and can be used to exchange ideas and views. Examples of such sites include, but are not limited to, MySpace, Twitter, Facebook, Instagram, Snap Chat, LinkedIn, YouTube, MSN, Forums, Bulletin Boards, Chatrooms, Instant Messenger and comment streams on public websites such as newspaper sites. The principles set out in this policy must be followed irrespective of the medium.
- 1.2 All employees are expected to comply with this policy and behave responsibly and professionally at all times whilst using social network sites. Employees should maintain a professional distance from pupils and therefore should not be involved in social networking with pupils either in or outside of the academy.
- 1.3 Whilst it is important that employees are able to use technology and related services effectively and flexibly, they must ensure that, when doing so, they do not make themselves vulnerable. This must also be balanced with the duty of the Headteacher and the Governing Body to safeguard children and the reputation of the academy.

2.0 Scope

- 2.1 This policy applies to all employees, including casual, agency staff, self-employed workers and volunteers.

3.0 Aims

- 3.1 This policy outlines the standards employees are required to observe when using social networking sites, and the action that will be taken in respect of any breaches of this policy.
- 3.2 It is not the intention of this policy to interfere with employees' personal lives but ask them to be mindful of the points outlined below (see 5.0) and not to bring the academy into disrepute with any inappropriate/offensive postings.
- 3.3 The policy aims to:
- a) Reinforce the need to use social networking sites safely and securely;
 - b) Ensure that employees are aware of the risks associated with the inappropriate use of social networking sites;
 - c) Safeguard employees in connection with the use of social networking sites and to ensure they do not put themselves or others in vulnerable situations;
 - d) Ensure that the Headteacher, the Governing Body and all employees maintain their duty to safeguard children and the reputation of the academy.

4.0 Responsibilities

- 4.1 **The Governing Body** must ensure that this policy is implemented and that both current, new employees and volunteers/students have access to, and are made aware of, this policy and their responsibilities.
- 4.2 **Headteachers/Line Managers** must be fully aware of this policy and ensure that they and all employees are aware of the policy and their own responsibilities. Employees must be made aware of the risks of using social networking sites and the possible implications to their employment if there is inappropriate use.
- 4.3 Advice from Human Resources can be sought where necessary, particularly where disciplinary procedures may need to be instigated.
- 4.4 **Employees** must behave responsibly and professionally at all times in connection with the use of social networking sites; both within the academy and outside of work, socialising etc. and must comply with this policy and co-operate fully with the academy's management in ensuring the implementation of this policy.

5.0 Use of Social Networking Sites

- 5.1 Access to social media sites for personal reasons during directed working hours is not permissible. Employees are expected to access these sites within their own personal time.
- 5.2 Employees may legitimately access social media sites for work purposes via academy information systems and equipment where this forms part of their role or with prior approval from the Headteacher.
- 5.3 Employees should be aware that when communicating via social networking sites anything said, shown or received could be made available, intentionally or unintentionally to a wider audience than originally intended.
- 5.4 Employees need to be aware that their reputation could be harmed by what others share about them online, such as being tagged into inappropriate posts, photographs, or videos.
- 5.5 Employees need to consider their own professional conduct online; certain behaviour could breach their employment code of conduct and therefore employees must follow the procedures below:
 - a) Employees must not access social networking sites for personal use via academy information systems or using academy equipment.
 - b) Employees must not accept pupils/students, parents/carers as 'friends' and must not approach pupils/students, parents/carers to become their friends on social networking sites. Such personal communication could be considered inappropriate and unprofessional.

- c) Employees must not befriend pupils (or approach pupils to become their friends) who have left the academy and are under the age of 18 years.
- d) Employees are reminded to regularly check the privacy settings on their social networking profiles, as they can change.
- e) Employees must not post inappropriate photographs (including photographs of pupils) on any social network site.
- f) Employees must not post any indecent remarks.
- g) If an employee receives messages on his/her social networking profile, which they think, could be from a pupil they must report this to their Line Manager/Headteacher, who will decide the appropriate action.
- h) Employees, should not make any reference to their place of work and must adhere to all guidelines in this policy. Identification of their place of work and profession on social media sites could potentially impact on the academy's reputation and the safety of employees.
- i) Employees must not disclose, on any social networking site, any information that is confidential to the academy and the Governing Body or disclose any personal data or information about any individual/colleague/pupil, which may breach the Data Protection Act/GDPR.
- j) Employees are advised to avoid posts or comments that refer to specific, individual matters related to the academy and members of its community on any social media accounts.
- k) Employees must not disclose any information about the academy and the Governing Body.
- l) Employees must not make defamatory remarks about the academy, colleagues, pupils, parents/carers or the Governing Body or post anything that could potentially bring the academy or the Governing Body into disrepute.
- m) Employees should not disclose any confidential information relating to his/her employment at the academy.
- n) Employees should take care to avoid using language/images on social network sites which others may find offensive.
- o) All employees should review their social networking sites regularly to ensure that information available publicly about them is appropriate and secure. This includes any personal images.

6.0 Breaches of the Policy

- 6.1 Although the academy/the Governing Body does not discourage employees from using social networking sites, all employees should be aware that the Headteacher/Governing Body will take seriously any circumstances where such sites are used inappropriately, including any usage that is considered to be online bullying or harassment.
- 6.2 Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils, parents/carers or other individuals connected with the academy, or another school/academy, could result in formal action being taken. This includes the uploading of images which might bring the academy into disrepute.
- 6.3 The Headteacher can exercise their right to monitor the use of the academy's information systems, including internet access, where they believe unauthorised use may be taking place; to ensure standards are maintained; to prevent or detect crime and to pick up messages when someone is away from work. If such monitoring detects the unauthorised use of social networking sites disciplinary action may be taken.
- 6.4 If any instances or allegations of the inappropriate use of social networking sites are brought to the attention of the Headteacher or a line manager, investigations will take place and **disciplinary action may be taken**. Any breach of this policy may constitute an act of gross misconduct.
- 6.5 Any breach of the policy by agency employees and self-employed workers will result in the arrangement for that particular worker being terminated and matters reported to the employment agency where appropriate.
- 6.6 There may be instances regarding the use of social networking sites where the academy or the Governing Body will be obliged to inform the police of any activity or behaviour about which there are concerns as to its legality.

7.0 Further Guidance

- 7.1 As professionals having daily contact with pupils/students, any contact on such sites with young people who may be friends of pupils/students is inappropriate.
- 7.2 Regular communications with parents/carers can be safely undertaken using the academy's secured sites such as: Face Book; Parent Pay; Twitter; You Tube and staff email

- 7.3 Instances or allegations of inappropriate use in relation to social networking with parents/carers of pupils will be investigated and may lead to disciplinary action.
- 7.4 Be aware that parents/carers and pupils may try to access your personal profiles. Ensure that privacy settings are secure and updated regularly.
- 7.5 In exceptional circumstances, where face to face communication is not possible, it may be necessary to undertake such meetings using on line systems such as virtual software, for example, Zoom or Microsoft Teams. Permission to record these meetings must be agreed by all parties prior to commencement. Confidentiality and professionalism must be maintained at all times.
- 7.6 Where a pupil is engaged in a virtual meeting, on school site or in their home setting, then appropriate adult supervision must be provided to ensure that the safety of the pupil is upheld. Any concerns must be reported immediately to the Designated Safeguarding Lead/Deputies or Senior Leader. Virtual meetings must be pre-arranged with a senior leader with reference to the clear, professional guidance outlined in the Code of Conduct and On Line Safety policies.

8.0 Equality Statement

- 8.1 This policy must be applied fairly to all employees irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation.

9.0 Additional Support

9.1

Childnet's Professional resources:

<http://www.childnet.com/teachers-and-professionals>

NCA-CEOP Ambassador course:

<https://www.thinkuknow.co.uk/professionals/training/ceop-ambassador-course/>

NSPCC and NCA-CEOP - Keeping Children Safe Online. an online introductory safeguarding course for anyone who works with children (2019 version):

<https://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-childrensafe-online-course/>

UK Safer Internet Centre training, advice and resources for teachers and professionals:

<https://www.saferinternet.org.uk/advice-centre/teachers-and-schoolstaff>

Online Safety Briefings:

<https://www.saferinternet.org.uk/training-events/online-safety-live-free-online-safetyevents>

DfE 'Teaching Online Safety in Schools' guidance
<https://www.gov.uk/government/publications/teaching-online-safety-in-schools>

DfE Statutory (September 2020) guidance for Relationships Education, Relationships and Sex Education (RSE) and Health Education
<https://www.gov.uk/government/publications/relationships-education-relationshipsand-sex-education-rse-and-health-education>

Childnet
<http://www.childnet.com/young-people>

PSHE Association/NPCC using police in the classroom guidance
<https://www.pshe-association.org.uk/policing>

UKCIS 'Education for a Connected World' framework:
<https://www.gov.uk/government/publications/education-for-a-connected-world>

UKCIS 'Using External Visitors to Support Online Safety Education: Guidance for Educational Settings'
<https://www.gov.uk/government/publications/using-external-visitors-to-supportonline-safety-education-guidance-for-educational-settings>

10.0 Parents' Links

10.1
Childnet:
<https://www.childnet.com/teachers-and-professionals/staff-led-online-safety-Where-to-go-for-more-support-presentations>

NCA-CEOP Thinkuknow:
<https://www.thinkuknow.co.uk/parents/>

Netware by NSPCC and O2:
<https://www.net-aware.org.uk>

Parent Info by NCA-CEOP and Parent Zone:
<http://parentinfo.org>

Parent Zone:
<http://parentzone.org.uk/>

Share Aware by NSPCC and O2:
<https://www.nspcc.org.uk/preventingabuse/keeping-children-safe/share-aware>

UK Safer Internet Centre:
<http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers>

Vodafone Digital Parenting resources:
<http://www.vodafoneigitalparenting.co.uk>