THE HEATH ACADEMY TRUST

Social Networking Policy

inspire transform together

Document Detail	
Category:	Safeguarding
Authorised By:	Trust Board
Version:	2026
Status:	Approved by Trust Board
Next Review Date:	January 2027

Version:	Date	Reason
2026	January 2026	Trust wide policy creation

Social Networking Policy

Contents

Contents **2**

Section 1: Introduction **3**
1.1 Objectives **3**
1.2 Scope **3**
1.3 Status **3**
1.4 Principles **4**

Section 2: Safer Social Media Practice in Schools **4**
2.1 What is social media? **4**
2.2 Overview and expectations **4**
2.3 Safer online behaviour **4**
2.4 Protection of personal information **5**
2.5 Communication between pupils / schools staff **5**
2.6 Social contact **6**
2.7 Access to inappropriate images and internet usage **6**
2.8 Cyberbullying **7**
2.9 Mobile Phone usage **7**
3.0 PREVENT **7**

Section 3: Link with other policies **8**

Section 4: Review of policy **8**

Section 5: Appendices **9**

Appendix A – Relevant legislation **9**

Appendix B - School Information **12**

Section 1: Introduction

1.1 Objectives

1.1.1 This document sets out the Heath Academy Trust policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for schools' staff in many ways. This document aims to:

- Assist schools' staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Reduce the incidence of positions of trust being abused or misused

1.1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in schools will always advise their headteachers of the justification for any such action already taken or proposed. Headteachers will in turn seek advice from the Schools' HR team where appropriate.

1.1.3 This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation listed at appendix A.

1.1.4 This policy has been agreed following consultation with the recognised trade unions and professional associations.

1.2 Scope

1.2.1 This document applies to all staff who work in the Heath Academy Trust schools. This includes teachers, support staff, supply staff, local school committee members, contractors, volunteers and trustees.

1.2.2 It should be followed by any adult whose work brings them into contact with pupils. References to staff should be taken to apply to all the above groups of people in schools. Reference to pupils means all pupils at the school.

1.2.3 This policy should not be used to address issues where other policies and procedures exist to deal with them. For example, any alleged misconduct which falls within the scope of the management of allegations policy requires the school to comply with additional child protection requirements as set out in that policy.

1.3 Status

1.3.1 This document does not replace or take priority over advice given by HR, the Safeguarding Unit or the School's Codes of Conduct, dealing with allegations of abuse, other policies issued around Safeguarding, E-Safety or IT issues (email, ICT and data protection policies), but is intended to both supplement and complement any such documents. This guidance has been agreed with the trade unions.

1.4 Principles

- Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Staff in schools should work and be seen to work, in an open and transparent way.
- Staff in schools should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

Section 2: Safer Social Media Practice in Schools

2.1 What is Social Media?

2.1.1 For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, Instagram, SnapChat and Whatsapp are perhaps the most well-known examples of social media but the term also covers other web-based services such as Blogs, video and audio Podcasts, Wikis, Message Boards, Photo document and Video sharing websites such as YouTube and Micro Blogging services such as X. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.

2.1.2 For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

2.2 Overview and expectations

2.2.1 All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the school's code of conduct. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

2.2.2 The guidance contained in this policy is an attempt to identify what behaviours are expected of schools' staff who work with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

2.2.3 School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

2.3 Safer online behaviour

2.3.1 Managing personal information effectively makes it far less likely that information will be misused.

2.3.2 In their own interests staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

2.3.3 All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate.

This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

2.3.4 Staff should never 'friend' a pupil at the school where they are working onto their social networking site.

2.3.5 Staff should never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil.

2.3.6 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.

2.3.7 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 or other individuals connected with the school, or another school, or the Trust could result in formal action being taken against them.

2.3.8 Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

2.3.9 Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or the Trust into disrepute.

2.3.10 Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the local authority.

2.4 Protection of personal information

2.4.1 Staff should ensure that they do not use school ICT equipment for personal use, e.g. camera or computers.

2.4.2 Staff should keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents.

2.4.3 Staff should never share their work log-ins or passwords with other people.

2.4.4 Staff should not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address should be used.

2.4.5 Staff should keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.

2.4.6 Staff are advised to understand who is allowed to view the content of their pages on the sites they use and how to restrict access to certain groups of people.

2.5 Communication between pupils/school's staff

2.5.1 Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries.

2.5.2 This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

2.5.3 It is the expectation that the school should provide a work mobile and e-mail address for communication between staff and pupils. Staff should not give their personal mobile numbers or personal e-mail addresses to pupils or parents.

2.5.4 Staff should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

2.5.5 Staff should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

2.5.6 Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers.

2.5.7 E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites. Internal e-mail systems should only be used in accordance with the school's policy.

2.6 Social contact

2.6.1 Staff should not establish or seek to establish social contact via social media/other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.

2.6.2 There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.

2.6.3 There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

2.7 Access to inappropriate images and internet usage

2.7.1 There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

2.7.2 Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

2.7.3 Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools and schools' staff need to ensure that internet equipment used by pupils have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

2.7.4 Where indecent images of children are found by staff, the police and local authority designated officer (LADO) should be immediately informed. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

2.7.5 Where other unsuitable material is found, which may not be illegal, but which raises concerns about that member of staff, either HR or the LADO should be informed and advice sought. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

2.8 Cyberbullying

2.8.1 Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

2.8.2 Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

2.8.3 If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

2.8.4 Staff may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process. Employees will also have access to the DCC staff counsellor, subject to funding being agreed.

2.8.5 Staff are encouraged to report all incidents of cyberbullying to their line manager or the headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

2.9 Mobile phone usage

2.9.1 Personal devices, including mobile phones, must not be accessed when in a prohibited area. A prohibited area includes any area of the school where children access. Staff are permitted to use their personal devices whilst in the staff room.

2.9.2 The school reserves the right to refuse staff and visitors permission to use their own device on school premises.

2.9.3 Personal devices must not be used to take photographs, video or audio recordings of pupils or staff.

3.0 PREVENT – A Community Safeguarding Programme

Prevent is about safeguarding people and communities from the threat of terrorism. Prevent is 1 of the 4 elements of CONTEST, the Government's counter-terrorism strategy. It aims to stop people becoming terrorists or supporting terrorism. At the heart of Prevent is safeguarding children and adults and providing early intervention to protect and divert people away from being drawn into terrorist activity.

If you see or hear something that could be terrorist related, call the Police Hotline on 0800 789 321.

If you are concerned about someone in your community, please contact the local police force by dialling 101 or if you require urgent police assistance, dial 999.

Section 3: Link with other policies

3.1.1 This policy should be read in conjunction with the following documents for schools:

Policy / Document	Relevance
E-Safety Policy	The standards outlined in the trust's E-Safety Policy document should be followed when using social networking sites.
Disciplinary Policy	Use of social networking sites which is not in accordance with this policy or the trust's policies may amount to misconduct or gross misconduct under the trust's disciplinary policy and procedure.
Remote Education Policy	This policy applies to children who are learning remotely
Anti-Bullying and Harassment Policy	Where use of social networking sites can be interpreted to constitute a form of bullying or harassment of another member of staff this may be dealt with under the anti-bullying and harassment policy in the first instance.
Equal Opportunities Policy	Use of social networking sites should at all times be in accordance with the trust's equal opportunities in employment policy.
Code of Conduct for all adults	The code sets out the standards of conduct expected of employees including maintaining the school's and trust's reputation, non-disclosure of confidential information and standards of behaviour expected.
Guidance for Safer Working Practice for Adults Who Work with Children and Young People	This document provides safeguarding guidance for all employees who work with children, young people and vulnerable adults, including guidance around communication with young people, photography and video.
Bring Your Own Device Policy	This policy sets out the arrangements for use of personal devices in school

3.1.2 All employees must adhere to and apply the principles of the policy in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

Section 4: Review of policy

4.1.1 Due to the ever-changing nature of information and communication technologies it is best practice that this policy be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

"We have reviewed this policy in line with the single equality seven strands: race/ethnicity, gender, religion/faith/belief, sexual orientation, transgender, age and rural isolation/exclusion/deprivation."

Section 5: Appendices

Appendix A – Relevant legislation

Schools staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer misuse act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data protection act 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of information act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious communications act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of investigatory powers act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, designs and patents act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal justice & public order act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and religious hatred act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from harassment act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of children act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual offences act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, fall in this category of trust). Any sexual intercourse with a child under the age of 16 commits the offence of rape.

Public order act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene publications act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human rights act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix B – School Information

This E-safety Policy applies to all schools within the Heath Academy Trust. Each school is listed below with the named individuals assigned to each role.

Oakhurst Community First and Nursery School

Headteacher:	Ann Clark
E-safety Officer:	Ann Clark
Chair of Local Schools Committee:	Holly Jones
Review Date: January 2026	Next Review: January 2027

Sixpenny Handley First and Nursery School

Head of School:	Laura Stone
E-safety Officer:	Laura Stone
Chair of Local Schools Committee:	Abi Carlyle-Clarke
Review Date: January 2026	Next Review: January 2027

St Ives Primary and Nursery School

Headteacher:	Laura Crossley
E-safety Officer:	Eve Moore
Chair of Local Schools Committee:	Mario Massimino
Review Date: January 2026	Next Review: January 2027

St James' CE First School and Nursery

Headteacher:	Jo Hudson
E-safety Officer:	Ben Spinks
Chair of Local Schools Committee:	Sean Cooper
Review Date: January 2026	Next Review: January 2027

St Mary's CE First School and Nursery

Head of School:	Sarah Corbett
E-safety Officer:	Holly Longman
Chair of Local Schools Committee:	Michelle Scott-Ashcroft
Review Date: January 2026	Next Review: January 2027

Three Legged Cross First and Nursery School

Head of School:	Anna Morris

E-safety Officer:	Alex Hustler
Chair of Local Schools Committee:	Catherine Stevens
Review Date: January 2026	Next Review: January 2027