Social Media and ICT Acceptable Use Policy

Version			2.0
Date			September 2017
Approved by Board of Directors			
Version	Date	Description	Revision author
1.0	September 2016	Created.	GAD
2.0	September 2017	Annual review	GAD

Contents

Page number

1 Introduction

1.1 The Trust recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide range of social media. However, employees' use of social media can pose risks to confidentiality and intellectual property, the Trust's reputation and can jeopardise compliance with legal obligations. Social media are web-based and mobile technologies that turn communication into active dialogue. There are many different types of social media channels, which attract specific audiences for different purposes. These include but are not limited to, LinkedIn, Facebook, Twitter, blogs, and specialist networking sites.

1.2 While recognising the benefits of these media within the educational environment, in order to minimise the above risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate purposes, this policy sets out the principles that all Trust employees must adhere to.

1.3 It is crucial that pupils, parents and the public at large have confidence in the Trust's decisions and services. The principles set out in this policy are designed to ensure that employees use social media responsibly so that confidentiality of data as well as the reputation of the Trust are safeguarded.

1.4 Employees must be conscious at all times of the need to keep their personal and professional lives separate.

1.5 This policy applies to all Trust employees, is non-contractual and may be amended at any time. Breach of this policy may potentially give rise to disciplinary action.

2 Scope of the Policy

2.1 This policy applies to the Trust's teaching and support staff including teacher trainees and other trainees.

2.2 This policy covers personal use of social media as well as the use of social media for official Trust purposes; including sites hosted and maintained on behalf of the Trust for example Virtual Learning Environments (VLEs).

2.3 This policy applies to personal web space such as social networking sites (for example *Facebook*,); blogs and micro-blogs such as *Twitter*, chat-rooms, forums, podcasts; open access online encyclopaedias such as *Wikipedia;* and content sharing sites such as *flickr* and *YouTube*. This list is not exhaustive. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

2.4 This policy applies to both the use of the Trust's ICT and communication equipment and also the use of personal devices by employees.
Examples of such devices include:

- Laptop and personal computers
- ICT network facilities
- Mobile phones
- USB sticks and other storage devices
- Image storage devices including cameras, camera phones and video equipment.

This list is not exhaustive

3 Aims of the Policy

This policy aims to:

3.1 Ensure that employees are aware of the risks associated with the inappropriate use of social networking sites and ICT facilities and understand the importance of using them safely and securely.

3.2 Safeguard employees to ensure they do not make themselves vulnerable to allegations through their use of social networking sites.

3.3 Ensure that the Trust maintains its duty to safeguard children, staff, and the reputation of the Trust and the wider community.

4 Legal Framework

4.1 The Trust is committed to ensuring that all employees provide confidential services that meet the highest standards. All individuals working on behalf of the Trust are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- the Data Protection Act 1998

4.2 Confidential information includes, but is not limited to:

- Information that identifies specific individuals, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- Trust business or records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and politically sensitive information

4.3 Employees should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988

4.4 The Trust could be held vicariously liable for acts of their employees in the course of their employment. For example, employees who harass co-workers online or who engage in cyber-bullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render the Trust liable to the injured party.

5 Responsibilities

5.1 The Trust shall ensure that all employees are made aware of this policy and shall ensure that the policy is implemented and procedures are in place to deal with non-compliance.

5.2 The Headteacher or appropriate senior leader shall ensure that all employees receive the relevant training and guidance in relation to the use of Social Networking and ICT.

5.3 The Headteacher will seek advice from HR where necessary.

5.4 The Headteacher or appropriate senior leader will ensure that any allegations made in relation to the above are investigated and any appropriate action is taken where necessary.

6 Related Policies

6.1 This policy should be read in conjunction with the following Trust policies

- Employee Code of Conduct
- Trust's Disciplinary Policy

7 Overarching Principles

7.1 You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the Trust and your personal interests.

7.2 You must not engage in activities involving social media which might bring the Trust into disrepute.

7.3 You must not represent your personal views as those of the Trust on any social medium.

7.4 You must not discuss personal information about pupils, other Trust employees or professionals you interact with as part of your job on social media.

7.5 You must not use social media and the internet in any way to attack, insult, and abuse or defame pupils, their family members, colleagues, other professionals, other organisations or the Trust.

7.6 You must be accurate, fair and transparent when creating or altering online sources of information on behalf of the Trust.

7.7 You must ensure, when contacting students for Trust business, appropriate monitored resources i.e. Trust mobile phone, Trust email system etc. are used as a safeguarding measure.

8 Personal Use of Social Media

8.1 Employees must not identify themselves as employees of the Trust in their personal web space. This is to prevent information on these sites from being linked with the Trust and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

8.2 The Trust does not expect employees to discontinue contact with their family members via personal social media once the Trust starts providing services for them. However, any information employees obtain in the course of their employment must not be used for personal gain or be passed on to others who may use it in such a way.

8.3 Employees must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

8.4 If employees wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the Trust and through official Trust sites created according to the requirements specified in section 9.

8.5 Employees must decline 'friend requests' from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils of any school who are not family members, they may discuss these in general terms in class where the pupils attend the school and signpost pupils to become 'friends' of the official school site if there is one.

8.6 Information employees have access to as part of their employment, including personal information about pupils and their family members, colleagues, and other parties and Trust corporate information must not be discussed on their personal web space.

8.7 Photographs, videos or any other types of images of pupils and their families or images depicting employees wearing clothing with school logos on must not be published on personal web space.

8.8 Trust/school email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

8.9 The Trust only permits limited personal use of social media during designated break points. However, employees are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be in the Trust's time. This is subject to such use:

- Not depriving pupils of the use of the equipment and/or
- Not interfering with the proper performance of employees duties

8.10 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

8.11 Employees are advised that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Employees should keep their passwords confidential, change them often and be careful about what is posted online. It is not appropriate to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

9 Using Social Media on Behalf of the Trust

9.1 Employees can only use official Trust/school sites for communicating with pupils or to enable pupils to communicate with one another.

9.2 Employees should seek permission from the Headteacher before creating an official Trust/school site explaining their business reasons for doing so.

9.3 Any official Trust/school sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

9.4 Employees must, at all times, act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

9.5 If you are contacted for comments about the Trust/school for publication anywhere, including in any social media outlet please direct the enquiry to the Headteacher.

10 Use of School ICT

10.1 Staff who use the Trust's ICT and communication systems:

- Must use it responsibly
- Must keep it safe
- Must keep passwords confidential and must report any breach of password confidentiality to the Headteacher or nominated ICT Co-ordinator as soon as possible
- Must report any known breaches of this policy, including any inappropriate images or other material which may be discovered on the Trust's/school's ICT systems
- Must report to the Headteacher or designated safeguarding officer any vulnerabilities affecting child protection in the Trust's/school's ICT and communications systems
- Must not install software on the Trust's/school's equipment unless authorised by the school's ICT Co-ordinator
- Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures
- Must ensure that it is used in compliance with this policy

10.2 Any equipment provided to a Trust employee is provided for their sole use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

11 Email and Communications Systems Usage

11.1 The following uses of ICT are prohibited, may amount to gross misconduct and could result in dismissal. Please see the Disciplinary Policy for further guidance.

- To make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that may deprave or corrupt those likely to read or see it
- To make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred
- For the purpose of bullying or harassment, or for or in connection with discrimination on the grounds of gender, race, religion, disability, age or sexual orientation

- For the publication and/or distribution of libellous statements or material which defames or degrades others
- For the publication of material that brings the Trust/school or its pupils or employees into disrepute
- For the publication and distribution of personal data without authorisation
- Where the content of the email correspondence is unlawful
- To participate in on-line gambling
- Where the use infringes copyright law
- To gain unauthorised access to internal or external computer systems (commonly known as hacking)
- To create or deliberately distribute ICT or communications systems viruses
- To record or monitor telephone or email communications without the express approval of the Trust. In no case will such recording or monitoring be permitted unless it has been established that such action is in full compliance will the relevant legislation i.e. the Regulation of Investigatory Powers Act 2000
- To participate in "chain" e-mail correspondence
- In pursuance of personal business or financial interests or political activities (excluding the legitimate activities of recognised trade unions)

12 Monitoring

12.1 The Trust's/school's IT department (where authorised by the Head teacher) reserves the right to monitor usage of its internet and email services without prior notification or authorisation from users.

A recent European Court of Human Rights case ruled that an employer was legitimately entitled to access an employee's social media messenger account. This was because the messages had been sent during working hours, from a work account and on a work device.

12.2 Therefore Users of the Trust's/school's email and internet services should have no expectation of privacy in anything they create, store, send or receive using the Trust's/school's ICT system. As such employees should not use the schools IT resources or communication systems for any matters that are private and confidential.

13 Breaches of the Policy

13.1 Any breach of this policy will be fully investigated and may lead to disciplinary action being taken against the employee/s involved in line with the Trust's Disciplinary Policy and Procedure.

13.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the Trust/school or any illegal act/s that render the Trust/school liable to third parties may result in disciplinary action or dismissal.

13.3 Contracted providers of the Trust's services must inform the Trust immediately if they become aware of any breaches of this policy so that

appropriate action can be taken to protect confidential information and limit the damage to the reputation of the Trust.

13.4 Under the Regulation of Investigatory Powers Act (2000) the Trust can exercise the right to monitor the use of the Trust's/school's information systems and internet access where it is believed that unauthorised use may be taking place, to ensure compliance with regulatory practices, to ensure standards of service are maintained, to prevent or detect crime, to protect the communications system and to pick up messages if someone is away from school.

13.5 In certain circumstances the Trust will be obliged to inform the Local Authority Designated Officer (LADO) and/or police of any activity where there are concerns that it may constitute a safeguarding issue or potentially involve illegal activity.

14 Review of the Policy

14.1 This policy will be reviewed on an annual basis and sooner if necessary due to changing technology or legislation.

Appendix A

Acceptable Usage of ICT and Social Media Form

This agreement relates to the Trust's Social Media and ICT Acceptable Use Policy outlined above. All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of this policy and to sign the agreement below.

You should sign two copies of this agreement. Please keep one copy for your records with this policy and return the second copy to school.

I confirm that I have been provided with a copy of the Trust's Social Media and ICT Acceptable Use Policy.

I have read understood and accept the Social Media and ICT Acceptable Use Policy and will abide by it.

Name: .....

Signed: ..... Date: .....