



# **Social Networking Policy & Procedure**

## **POLICY**

The Trust recognises that employees have right to access social networking sites for personal communications. This policy gives guidance and advice on how employees should conduct themselves and control and monitor information stored on such sites.

### **Scope and Purpose**

This procedure applies to all employees of the Trust.

Social networking sites allow users to build on-line profiles, share information, music and photographs, however users are reminded that information uploaded onto such sites, may be viewed by others even if it appears to be “private” or is stored within a closed profile or group. Information that you do not wish others to view should not be uploaded in such a public domain and staff should ensure that their security settings are maintained at an appropriate level.

### **1. Introduction**

The Trust is committed to ensuring that all staff are aware of their responsibilities in connection with the growing use of social networking sites. It recognises that the use of such sites have become a very significant part of life for many people. They provide a positive way to keep in touch with friends and colleagues, and can be used to exchange ideas and thoughts on common interests. Examples of such sites include, but are not limited to, blogs (short for web log), Twitter, Google Plus, Flickr, MySpace, Facebook, Bebo, YouTube, Windows Live Spaces, MSN, forums, bulletin boards, multiplayer online gaming, chat rooms and instant messenger’, this list however is by no means exhaustive.

Staff are expected to keep a professional distance from pupils and there should be a clear separation of the private social lives of staff and that of pupils. There is no need for social networking to go on between staff and pupils and there is no clear educational benefit. Staff should also ensure that their relationships and interactions with colleagues when using social networking sites remain appropriate and professional.

It is important that staff are able to use technologies and services effectively and flexibly whilst ensuring that they do not make themselves vulnerable. However, it is also important to ensure that this is balanced with the Governing Body’s duty to safeguard children, the reputation of the schools within the Trust and the Trust, and the wider community.

## **2. Aims**

The policy aims to:

- Enable employees to use social networking sites safely and securely;
- Ensure that employees are aware of the risks associated with the inappropriate use of social networking sites;
- Safeguard employees in connection with the use of social networking sites and ensure they do not make themselves vulnerable;
- Ensure the Governing Body maintains its duty to safeguard children, the reputation of the school, the Trust and the wider community.

## **3. Legislation**

The following legislation must be considered when adhering to this policy:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Equality Act 2010

## **4. Responsibilities**

### **4.1 The Governing Body (in conjunction with the Trust) shall:**

- Ensure this policy is implemented and procedures are in place that deal with the use of social networking sites;
- Ensure that all employees have access to this policy and that new employees are made aware of it.
- Ensure that all employees are aware of the Trusts Information Governance Policy

### **4.2 Head Teachers/Line Managers shall:**

- Be familiar with this policy and guidelines and ensure that employees understand the policy and their own responsibilities;
- Take responsibility for ensuring that all new employees are made aware of the policy when they commence their employment;
- Ensure that staff are aware of the risks of the use of social networking sites and the possible implications of the inappropriate use of them;
- Instigate disciplinary procedures where appropriate to do so;

- Seek advice where necessary from the Head of Operations and the HR & Governance Manager on the approach to be adopted if they are made aware of any potential issue.
- Be familiar with the Trusts Information Governance Policy and ensure that employees understand the policy and their own responsibilities.
- Ensure that their own personal conduct and interaction with other colleagues when using social networking sites remains appropriate and sets a positive example to other staff at all times.
- Ensure staff are aware that if any instances of the alleged inappropriate use of social networking sites are brought to the attention of the Headteacher, the disciplinary procedure will apply.

#### **4.3 Staff shall:**

- Behave responsibly and professionally at all times in connection with the use of social networking sites;
- Co-operate with management in ensuring the implementation of this policy.
- Be responsible for all contents/ comments on their own site
- Ensure all security settings are set at an appropriate level
- Be familiar with the Trust's Information Governance Policy.
- Ensure that caution is exercised when accessing sites to ensure that Network Security is not compromised

#### **4.4 The Trust shall:**

- Provide the necessary professional advice and support to the Governing Body and all Trust staff when required.
- Liaise with the Safeguarding Unit with regards to any potential Child Protection concerns that may arise, if necessary.
- Follow the Managing allegations against Staff (MAAS) protocol in conjunction with the relevant Senior member of staff in School/Trust
- Take appropriate action, which in some cases may result in suspension should the conduct be construed as gross misconduct.

There may be instances where the School or Trust will be obliged to inform the police of any activity or behavior for which there are concerns as to its legality.

### **5. Use of Social Networking Sites**

For employees' own security all communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore advised that staff follow the following procedures:

- Staff must adhere to the Trusts own usage policy in relation to accessing social networking sites for personal use via school/trust information systems or using school equipment;

- Staff must not accept pupils as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations;
- Staff are advised not to be friends with recent pupils. The potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking;
- Staff should not place inappropriate photographs on any social network space;
- Staff should not post indecent remarks;
- If a member of staff receives messages on his/her social networking profile that they think could be from a pupil, or becomes exposed to any information that relates to the School/Trust or another member of staff, they must report it to their Line Manager/Headteacher and contact the internet service or social networking provider so that they can investigate and take the appropriate action;
- Staff should not write about their place of work/ colleagues and pupils. Should a member of staff do so he/she will be in breach of this policy.
- Staff must not disclose information or work such as lesson plans, presentations, project work etc. that could be considered to be the intellectual property of the Trust
- Staff must not disclose any information that is confidential to the school/Trust or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act;
- Staff must not disclose any information about the school/Trust that is not yet in the public arena;
- In no circumstances should staff post photographs of pupils;
- Staff should not make defamatory remarks about the school/colleagues/pupils or the Trust or post anything that could potentially bring the School/Trust into disrepute;
- Staff should not disclose confidential information relating to his/her employment at the School/Trust or indicate any political allegiances
- Care should be taken to avoid using language which could be deemed as offensive, derogatory or inappropriate to others.
- Staff should not post information or comments or engage in any discussions that could be interpreted as bullying, harassment or discrimination of any description.
- Staff should not join any online groups that could be considered to condone or promote inappropriate behaviours or post inappropriate content.

## **6. Breaches of the Policy**

The Trust does not discourage staff from using social networking sites and appreciates that there may be occasions effective business tool. However, all staff

should be aware that the Trust will take seriously any occasions where the services are used inappropriately. If occasions arise of what could be deemed to be online bullying, harassment, defamation or misconduct of any description, these will be dealt with in the same way as other such instances occurring “offline”.

Under the Regulation of Investigatory Powers Act 2000 (RIPA), the Headteacher/Chief Executive Officer can exercise his/her right to monitor the use of the school’s information systems and internet access where he/she believes 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 communication system and to pick up messages when someone is away from School/Trust. If any such monitoring detects the unauthorised use of social networking sites disciplinary action will be taken.