

# IES BRECKLAND

## SOCIAL NETWORKING POLICY

Approved by the Governing Body October 2015

Chair of Governors:



## **General**

This policy on social networking websites is in addition to the School's existing policy on email and internet use or Acceptable Use Policy. It takes account of the ACAS guidance on Social Networking.

In this policy 'staff' means employees, volunteers (including governors), agency staff or anyone working within the school and using the school's IT equipment.

As staff are aware, the internet is provided (primarily) for school use. We recognise however, that many employees may rarely use the internet for personal purposes while in school. We also recognise that many employees participate in social networking on websites such as Facebook, Twitter, MySpace, Bebo and Friendster outside of work.

The purpose of this policy is to outline the responsibilities of staff using the internet to access social networking websites.

This policy applies to all staff using the school's IT equipment.

## **Personal use of the internet**

The school restricts and monitors access to social networking websites from its computers at all times. Access will only be allowed where use of such websites is for school purposes.

## **Personal conduct**

The school respects staff's right to a private life. However, the school must also ensure that confidentiality, its pupils, employees, volunteers, and its reputation are protected. It therefore requires staff using social networking websites to:

- use caution when posting information on social networking sites and blogs
- refrain from identifying themselves as working for the school
- ensure that they do not conduct themselves in a way that is detrimental to the school; and
- take care not to allow their interaction on these websites to damage working relationships between members of staff, pupils at the school and their families, and other stakeholders or working partners of the school

If staff become aware of inappropriate material/comments they should notify the Principal as soon as possible, and if possible provide print outs of the comments made or of the pictures displayed.

Staff must not be 'friends' or communicate with, students on any social network sites or similar websites, including, but not limited to, 'Facebook', 'Myspace', 'Twitter' etc. If any student makes contact with any staff member, they must notify the Principal as soon as possible without making a response. Similarly, if any member of staff or individual

associated with the school makes unintended contact with a pupil, it must be notified to the Principal as soon as possible. In the absence of the Principal, a member of the Leadership Team must be contacted. The Principal can then deal with the situation as appropriate.

It is recommended that Staff do not 'like' the school's 'Facebook' page, as this could leave them open to their profile being viewed by other members of the group including students and parents. Staff who use social networking sites like 'Facebook' must ensure they protect themselves through using appropriate security filters.

Staff are reminded that bullying and harassment against any other member of staff via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the schools' normal bullying and harassment or disciplinary policies, as appropriate and may also be treated as a criminal offence.

Employees that post defamatory statements that are published on the internet may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by employees could mean the school is vicariously liable for those statements if done in the course of employment, even if performed without the consent or approval of the school. The school takes these acts seriously and disciplinary procedures will be invoked if any such defamatory statements are made by its employees, which may lead to dismissal.

In the case of Governors, whilst volunteers and not subject to disciplinary procedures, advice and guidance will be taken.

### **Monitoring of internet access at work**

We reserve the right to monitor staffs' internet usage, but will endeavour to inform an affected individual when this is to happen and the reasons for it. We consider that valid reasons for checking a member of staff's internet usage include suspicions that they have:

- been spending an excessive amount of time viewing websites that are not work-related; or
- acted in a way that damages the reputation of the school and/or breaches confidentiality
- contravened safeguarding policies or given cause for concern about their suitability to work with children

The school reserves the right to request information regarding members of staff's use of the internet from our Internet Service Provider (ISP).

### **Disciplinary action**

If the school monitors staffs' internet use to ensure that it is in accordance with this policy, access to the web may be withdrawn in any case of misuse of this facility.

If appropriate, disciplinary action will also be taken in line with the school's disciplinary policy.

### **Security and identity theft**

Staff should be aware that social networking websites are a public forum, particularly if the individual is part of a "network". Staff should not assume that their entries on any website will remain private. Staff should never send abusive or defamatory messages.

Staff must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, staff must:

- ensure that no information is made available that could provide a person with unauthorised access to the school and/or any confidential information; and
- refrain from recording any confidential information regarding the school on any social networking website

Publishing of information on social network sites should be assumed to be in the public domain as this will be assumed in all cases of breach of the policy.

We ask all staff to consider the following before posting information or images on social networking sites:

- Think carefully before posting information – would you want your employer or a potential employer to see it
- Think carefully about who might see this, i.e. parents, pupils, the wider community, and what you do and don't want them to see
- Review your information regularly – what may have seemed like a good idea at the time may not seem such a good idea some months or years later