The Brooksbank School Sports College

E-Safety: Social Networking Policy

Version Number	4.0
Date of Issue	February 2018
Date Approved	February 2018
Date for Review	February 2021
Approved by	Head & Safeguarding Governor
SLT Member Responsible	Director of Finance & Resources

POLICY ON THE USE OF SOCIAL NETWORKING SITES – STAFF GUIDANCE

(To be read in conjunction with the e-Safety Policy, e-Safety Guide and the ICT Acceptable Use Policies)

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

General

Access to the internet via the school's IT equipment is provided (primarily) for school use. We recognise however, that many employees may occasionally access 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, LinkedIn and Friendster outside of work (hereby referred to as social networking websites).

The purpose of this policy is to outline the responsibilities of staff using the internet to access social networking websites and applies to all staff using the school's IT equipment.

This policy on the use of social networking websites is in addition to the School's existing policy on e-Safety and the Acceptable Use Policy. It takes account of the ACAS guidance on Social Networking. In addition, other relevant professional standards, principles and codes of conduct applied by the school will sit alongside this policy. These include: Teachers' Standards, National Occupational Standards for Supporting Teaching Learning and the 'Nolan Principles'. The school expects all staff to abide by these standards, as applicable to their role.

Monitoring use of the Internet and associated activities

All staff should be aware that use of the ICT network, including access to the internet is monitored on a regular basis. Access to social networking websites during working hours will only normally be allowed where use of such websites is for school purposes.

In addition, more forensic investigation could take place where there are concerns around the safeguarding agenda, possible cyber-bullying or a detrimental effect on the school's reputation.

Personal conduct

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

- use caution and act responsibly when posting information on social networking sites and strongly advise from identifying themselves as working for or in any other way connected to the school
- ensure that they do not conduct themselves in a way that conflicts with their professional code of conduct, or is otherwise detrimental to the school;
- take care not to allow their interaction on these websites to damage working relationships between members of staff, students and their families, and other stakeholders or working partners of the school.

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

Staff should not be 'friends' or communicate with, students on any social networking sites. If any student directly makes contact with any staff member, the staff member should notify the Headteacher 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, this must be notified to the Head Teacher as soon as possible. In the absence of the Head Teacher, the Deputy or Assistant Head or a member of the SLT must be contacted. The Headteacher can then deal with the situation as appropriate.

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' disciplinary policies, as appropriate and may also be treated as a criminal offence.

Employees that post defamatory statements about the school or their colleagues on the internet may be legally liable for any damage to the reputation of the individuals concerned. In addition, as a representative of the school, any statement made by employees could mean the school is vicariously liable for those statements even if they have acted 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. .

In the case of Governors, Trustees or Directors and volunteers, whilst these individuals are not subject to disciplinary procedures, advice and guidance will be taken as necessary, in relation to referral and sanctions under appropriate governing body procedures.

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". Any information posted on social network sites should be assumed to be in the public domain and this will be assumed in all cases of breach of the policy.

Staff should not assume that their entries on any website will remain private. Staff should never send abusive or defamatory messages.

Social networking websites allow people to post detailed personal information which can form the basis of security questions and passwords. Staff should be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. In addition, staff must ensure that no information is made available that could provide a reader with unauthorised access to the school and/or any confidential information;

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

- Think carefully about who might see it, i.e. parents, pupils, the wider community – do you really want them to be able to 'see' it
- Review your information regularly and do not post information 'in the heat of the moment' – what may have seemed like a good idea at the time may not seem such a good idea the next day or some months or years later.
- Think carefully before posting information – would you want your employer or a potential employer to see it?