Thames View Infants
Social Networking Policy

Introduction

This policy, which applies to all Staff, Advisers and Trustees, should be read in accordance with the School's Acceptable Use (of the Internet) and e-Safety Policy; and is underwritten by the School's Whistleblowing and Safeguarding Policies.

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The two with the widest use are Facebook and Twitter. The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This policy and associated guidance is to protect staff and advise school leadership on how to deal with potential inappropriate use of social networking sites. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. The purpose of this policy is to ensure:

- that School is not exposed to legal and governance risks;
- that the reputation of the School is not adversely affected;
- that our users are able to clearly distinguish where information has been provided via social networking applications, that it is legitimately representative of the School;
- protocols to be applied where employees are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include but are not limited to:

- blogs i.e. blogger;
- Online discussion forums, for example Facebook, SnapChat, Instagram;
- Media sharing services for example YouTube;
- 'Micro-blogging' application for example Twitter;
- 'DM's (direct messages) within applications such as Instagram or Facebook.

Scope

This policy covers the use of social networking applications by all school stakeholders, including, employees, Governors and pupils. These groups are referred to collectively as 'school representatives' for brevity.

The requirements of this policy apply to all uses of social networking applications which are used for any school related purpose and regardless of whether the School representatives are contributing in a personal capacity or an official capacity to social networking applications.

Access to Social Networking Sites

At the time of writing, teachers and key staff are permitted to have official Twitter accounts. There is an official YouTube channel, maintained by the ICT Network Manager. However, this might include internal forums for staff and outward facing forums for school activities/clubs etc. Restricted

access for 'Official' work purposes is permitted for the above named applications, where explicit permission has been given by the Headteacher.

The use of social networking applications in work time for personal use is not permitted.

School Managing Social Networking Sites ('Official Use')

It is important to ensure that employees, members of the public and other users of online services know when a social networking application is being used for official School purposes. To assist with this, all employees must adhere to the following requirements:

- All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head teacher first.
- Only use an official (i.e. not personal) email addresses or account name which will be used for official purposes. Staff must not use "personal" accounts to comment on "official" school business.
- The School's logo and other branding elements should be used where appropriate to indicate the School's support. The School's logo should not be used on social networking applications which are unrelated to or are not representative of the School's official position;
- Employees should identify themselves as their official position held within the School on social networking applications; e.g. through providing additional information on user profiles;
- Employees should ensure that any contributions on any social networking application they make are strictly professional, remain confidential, uphold the ethos and reputation of the School and do not give rise to bringing the school into disrepute. (General 'everyday' "common sense" guidance for conduct professional conduct applies);
- Staff should not spend an unreasonable or disproportionate amount of time during the working day developing, maintaining or using sites;
- Employees must not promote or comment on personal, political, religious or other matters;
- Pictures of children taken should follow the guidance set out within the school's Acceptable Use Policy. In particular, those staff permitted to use their own mobile devices to illustrate a School-authorised Twitter account must ensure that all pictures of children are removed from that device at the end of the school day.
- Employees should be aware that sites will be monitored.
- Staff may approve "friendship"/"follow" requests from parents within School-authorised Twitter and YouTube account/s, but not pupils.

Personal Social Networking Sites

All employees of the School should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, Data Protection and Freedom of Information legislation and the Safeguarding Vulnerable Groups Act 2006. Employees must also operate in line with the School's Equality Plan.

Any communications or content published on a social networking site which is open to public view, may be seen by members of the school community. Employees hold positions of responsibility and

are viewed as such in the public domain. Inappropriate usage of social networking sites by employees can have a major impact on the employment relationship. Any posting that causes damage to the School, any of it employees or any third party's reputation may amount to an investigation under the LBBD Disciplinary Procedures for School Staff (which could result in gross misconduct and potentially, dismissal).

When contributing to personal posts, staff should be mindful of the audience, not disclose sensitive or confidential information about school and not risk bringing the school into disrepute.

Employees should not use personal sites for any professional activity. The School reserves the right to require the closure of any applications or removal of content published by employees which may adversely affect the reputation of the School or put it at risk of legal action.

Anyone who becomes aware of inappropriate postings on social networking sites, must report it to their line manager as soon as possible. The line manager will then follow the disciplinary procedure. If an employee fails to disclose an incident or type of conduct relating to social networking sites, knowing that it is inappropriate and falls within the remit of this policy, then that employee may be subject to the disciplinary procedure.

1. Posting inappropriate images

Indecent images of any employee that can be accessed by students, parents or members of the public are unacceptable and can lead to child protection issues as well as bringing the School into disrepute. Staff must not post pictures of school children within personal sites.

2. Posting inappropriate comments

It is unacceptable for any employee to discuss pupils, parents, work colleagues or any other member of the school community on any type of social networking site. Reports about oneself may also impact on the employment relationship for example if an employee is off sick but makes comments on a site to the contrary.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Thames View Infants expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with other related school policies.

3. Social interaction with pupils (past and present)

Employees should not interact with or engage in conversation whatsoever with any child under the 18 that they come into contact within their professional capacity on any personal social networking site. This may include for example, pupils and their siblings or students on placement or work experience, past or present. Offers of assistance to a pupil with their studies via any social networking site are inappropriate and also leaves the employee vulnerable to allegations being made. Should an employee become aware of an underage person using social networking sites, (Facebook and Whatsapp for example, have this set at 13 years), then they should report this to the Headteacher.

4. Making Friends

Employees should be cautious when accepting new people as friends on a social networking site where they are not entirely sure who they are communicating with. We recommend that school staff ensure that personal social networking sites are set at "private". We also strongly advise that school staff are mindful of the potential audience when posting comments and sharing information/posts. Whilst we acknowledge that it might not be always possible to do so in a context where staff live local to a school community, we recommend not listing parents as approved contacts. Being mindful of this guidance will reduce the risk of employees being vulnerable to allegations being made.

5. We advise that Personal Social Networking Applications should not:

- be used to publish any content which may result in actions for breach of contract, defamation, discrimination, breaches of copyright, data protection, breach of confidentiality, intellectual property rights or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature including any radicalised, terrorist or extremist political or religious viewpoint (or association with such groups which may give reason to undermine the up-keeping of British values) that may bring the School or the local authority into disrepute. Some examples are given in Appendix A;
- be used for party political purposes of specific campaigning purposes as the local authority is not permitted to publish any material which 'in whole or part appears to affect public support for a political party' (LGA 1986);
- be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- be used in an abusive or hateful manner;
- be used for actions that would put other employees in breach of the Code of Conduct Policy;
- be in breach of the School's disciplinary and equal opportunities policies.
- be used to discuss or advise any matters relating to school matters, staff, pupils or parents

6. Additional Responsibilities governing the personal use of Social Networking Applications:

- Employees should not identify themselves as a representative of the school.
- References should not be made to any staff member, pupil, parent or school activity/event.
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.
- It is illegal for an adult to network online, giving their age and status as a child.

- Anyone with evidence of pupils or adults using social networking sites in the working day, should contact the named Child Protection Lead in School.

Where individuals from partner organisations are involved and are acting on behalf of the School, they will also be expected to comply with the relevant policies.

General Guidance/Protection for Pupils/Visitors/Older Students on using Social Networking Sites

- No pupil under 13 should be accessing social networking sites. There is a mechanism on Facebook where pupils can be reported via the Help screen.
- No pupil may access social networking sites at school at any time of day.
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens
- Please report any improper contact or cyber bullying in confidence as soon as it happens. We have a zero tolerance to cyber bullying
- We are aware of the Potential for Harmful Online Challenges and Online Hoaxes and if this happens, would share information with Parents/Carers, including where to get help or information.

Cyber Bullying

- The signs and effects of Cyber Bullying will be taught during ICT and PSHE lessons and within Assemblies, including how to whistleblow this to an adult. By adopting the recommended no use of social networking sites on school premises, Thames View Infants protects themselves from accusations of complicity in any cyber bullying through the provision of access.
- Parents should be clearly aware of the school's policy of access to social; networking sites.
- Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

Violation of this policy could result in disciplinary action being taken against the employee under the LBBD Code of Conduct Policy for School Staff and/or result in a Safeguarding Investigation.

Appendix A - Examples of unacceptable behaviour using Social Networking Sites

1. Breach of contract

There is an implied term of mutual trust and confidence between employer and employee in all employment contracts. A very negative and damaging posting or communication on a social networking site about the School or colleagues may entitle the Head teacher/line manager to decide that this term has been broken. Such conduct would be subject to the School's disciplinary procedure.

Emails are capable of forming contractual documents. Contracts can easily be formed by careless emails and non-compliance with the terms of any such contracts will render an organisation liable for a breach of contract claim. Emails tend not to be subject to the same safeguard procedures as paper documents which are often checked before they are signed off.

2. Defamation

If an employee places defamatory information or material on a social networking site such as bad mouthing another colleague or a pupil of the School, such conduct would be subject to the School's disciplinary procedure and could lead to the employee's dismissal.

3. Discrimination

The School's recruitment and selection policy provides the correct and proper procedures to be used in the recruitment and selection of staff. Candidates should be selected on the basis of testable evidence provided on application forms and through the selection process and references as provided by the applicant. Under no circumstances should information from social networking sites be used to make selection decisions. Such action could result in expensive discrimination claims. For example - not all candidates will have profiles on social networking sites and using information from this source may be seen as giving an unfair advantage or disadvantage to certain candidates, possibly discriminating against younger people who are likely to use social networking sites more often.

Many forms of discrimination claims, including harassment claim can occur via emails, If an employee places discriminatory material about another employee, a member of the Governing Body, parents, children, young people, and vulnerable adults, this could amount to bullying or harassment of that individual. The School may be vicariously liable for such acts unless it took such steps that were reasonably practicable to prevent material being placed on a site. Where an employee carries out an act of harassment or discrimination in the course of their employment, the School is vicariously liable for that act even when the act is unauthorised. Once an issue of email harassment has been raised and the harasser identified, immediate action should be taken to stop the harassment and instigate the disciplinary procedure while supporting the harassed employee.

4. Breach of Health and Safety

For example, an internet video clip of employees performing stunts wearing the organisation's uniform. When information like this is found, the School should follow the company's disciplinary procedure to investigate the possibility of a breach of health and safety legislation on the part of the employee. If a School is aware of this and fails to investigate there may be liability for personal injuries in the law of negligence.

Thames View Infants
Social Networking Policy

Dear Staff Member;

Reference: Use of Internet – Social Networking Sites

As the use of the internet and particularly social networking sites such as 'Facebook' becomes more widespread the local authority has become increasingly aware of the potential problems this can create for staff employed in schools or environments where they have close contact with children or vulnerable adults.

The School's Social Networking Policy sets out clear guidance in this complicated area. I am writing to all staff to help them ensure they are aware of the possible risks connected with the use of social networking sites arising as a result of their employment at a school.

Recently, the Human Resources Department at LBBD have had to investigate the inappropriate use of these sites. Accordingly, it is strongly advised that all staff should read the School's Social Networking Policy and consider the following points to protect themselves when using any social networking web sites.

1. Confidentiality – If any information known to you as a result of your employment at the school or any personal details relating to either pupils and their families or information regarding other staff employed by the school appears on a social networking or indeed any area of the internet this could be considered to be a breach of your duty to maintain confidentiality. It is also possible that you could be in breach of the Data Protection Act. This Act protects all personal data whether in electronic or paper format.

2. Reputation – There have been a number of disciplinary cases in public and business organizations arising from comments recorded on social networking websites. As employees working in organizations where we are already required to undergo enhanced CRB checks there is an expectation that the face we show to the rest of the world even outside of our roles in school should inspire respect and confidence. In some cases for example, staff had put their holiday photos on their Facebook sites but due to incorrect security settings pupils were able to access them and use them in a manner that caused the staff concerned a great deal of embarrassment and reflected badly on the reputation of their school.

3. Inappropriate Contact – In times when the internet is recognized as a place where adults do have inappropriate contact with children it is important for staff to ensure that they do not place themselves in a position of vulnerability.

The current general advice from LBBD regarding this issue is that ideally staff should avoid all use of social networking sites but if you do decide to use these services to carefully consider the points set out above. Ensure that you do have the correct security settings on your site and review the status of anyone whom you allow to access your site. Human Resources at LBBD have stressed that it is the personal responsibility of all staff to ensure they act responsibly in this area and to seek advice at the earliest possible opportunity if there appears to be a problem.

4 Whistleblowing – You will immediately report any illegal, inappropriate or harmful material or incident you become aware of to the appropriate person, including concerns you have regarding the radicalisation of pupils and colleagues.

As this is such an important issue I would be grateful if you could acknowledge receipt of this letter by completing the tear-off slip below and returning it to the School Office.

If you have any concerns arising from the contents of this letter I will be pleased to help.

Yours sincerely

Paul Jordan
Headteacher

==========

Name…….. Date……..

I confirm that I have received and read the letter 'Use of the Internet – Social Networking Sites" and read the School's Social Networking Policy.

Signed……..