Policy:	Social Media
Person(s) responsible for updating the policy:	Chief Executive Officer
Date Approved:	Board of Directors on 7 July 2016
Date of Review:	Every 3 years
Status:	Non Statutory

Tudor Park Education Trust oversees this policy but the local governing body of each academy or school within the Trust is responsible for the implementation of the policy.

This policy should be read with reference to the following policies:

- Safeguarding and Child Protection
- Data protection policy.
- ICT and use of the internet and intranet by staff policy.
- ICT and use of the internet and intranet by pupils policy.
- E-safety policy (useful for legal references)..
- Staff email policy.
- Bring Your Own Device policy

Education Update June 2013ii 'offensive social networking' may also be of interest as may *Social networking – guidelines for members (* NASUWT 2012). www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking/NASUWT_007513.

ASCL has also produced a useful guidance paper (ASCL Guidance Paper 117: Social Networking and Social media).

Background

As far as schools are concerned the term social media refers to any interactive platform, including social networks, internet forums and blogs. Given the rapid expansion of social media, it is impossible to list all possible types of media. While acknowledging the benefits of social media and the internet it is also important to recognise that risk to the safety and well-being of users is ever-changing and that the misuse/abuse of these facilities can range from inappropriate to criminal and schools need to have mechanisms in place to deal with misuse of social media. Misuse can be summarised as:

Contact

Commercial (tracking, harvesting personal information).

Aggressive (being bullied, harassed or stalked).

Sexual (meeting strangers, being groomed).

Values (self-harm, unwelcome persuasions).

Conduct

Commercial (illegal downloading, hacking, gambling, financial scams).

Aggressive (bullying or harassing another).

Sexual (creating and uploading inappropriate material).

Values (providing misleading info or advice).

Content

Commercial (adverts, spam, sponsorship, personal information).

Aggressive (violent/hateful content).

Sexual (pornographic or unwelcome sexual content).

Values (bias, racism, misleading info or advice).

SOCIAL MEDIA POLICY

Introduction

For the purposes of this policy, social media refers to any interactive platform, including social networks, internet forums and blogs. Given the rapid expansion of social media, it is impossible to list all possible types of media. All online activity is covered by this policy and should follow these guidelines in relation to any social media that they use, both at work and in their personal situation.

While acknowledging the benefits of social media and the internet it is also important to recognise that risk to the safety and well-being of users is ever-changing and that the misuse/abuse of these facilities can range from inappropriate to criminal and this policy in place to deal with any misuse of social media.

Objectives and targets

This policy applies to teachers, support staff, governors, volunteers and all who work on the school site.

This policy takes account of all the appropriate legislation and sets out to:

- Assist those who work with pupils to work safely and responsibly, to monitor their own standards of behaviour and to prevent the abuse of their position of trust with pupils.
- Offer a code of practice relevant to social media for educational, personal and recreational use.
- Advise that, in the event of unsafe and/or unacceptable behaviour, disciplinary or legal action (including gross misconduct leading to dismissal) will be taken if necessary in order to support safer working practice and minimise the risk of malicious allegations against staff and others who have contact with pupils.

Action plan

Use of social media within school

Staff have limited access to social media websites from the school's computers. Staff may use their own devices to access social media websites while they are in school, outside of session times (refer to Use of Personally Owned Devices Policy). Excessive use of social media, which could be considered to interfere with productivity, will be considered a disciplinary matter.

Staff should assume that anything they write (regardless of their privacy settings) could become public so should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Any use of social media made in a professional capacity must not:

- Bring the school into disrepute.
- Breach confidentiality.

- Breach copyrights of any kind.
- Bully, harass or be discriminatory in any way.
- Be defamatory or derogatory.

Where staff are blogging or contributing to social media with reference to the school they should consider seeking authorisation from the Principal.

Use of social media outside of school

The school appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the school, opinions they express could be considered to reflect the school's opinions and so could damage the reputation of the school. For this reason, staff should avoid mentioning the school by name, or any member of staff by name or position. Opinions offered should not to bring the school into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

General considerations

When using social media staff and others should:

- Never share work log-in details or passwords.
- Keep personal phone numbers private.
- Never give personal email addresses to pupils or parents.
- Restrict access to certain groups of people on their social media sites and pages.
- Ensure that the information you are displaying is accurate.
- Must never upload photos of students, or photos with students in a personal capacity.

Those working with children have a duty of care and are therefore expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and pupils both within and outside of school. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties eg for 'cyber-bullying' or identity theft.

- Staff should not make 'friends' of pupils at the school because this could potentially be construed as 'grooming', nor should they accept invitations to become a 'friend' of any pupils.
- Staff should avoid making 'friends' with ex-pupils of the school.
- Staff should also carefully consider contact with a pupil's family members because this may give rise to concerns over objectivity and/or impartiality.
- Staff should keep any communications with pupils transparent and professional and should only use the school's systems for communications.

- If there is any doubt about whether communication between a pupil/parent and member of staff is acceptable and appropriate a member of the senior management team should be informed so that they can decide how to deal with the situation.
- Before joining the school new employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

Misuse of social media

While acknowledging the benefits of social media and the internet it is also important to recognise that risk to the safety and well-being of users is ever-changing and that the misuse/abuse of these facilities can range from inappropriate to criminal. Misuse is summarised at the start of this policy into Contact, Conduct and Content.

Disciplinary action

Any breach of this policy may lead to disciplinary action under the school's disciplinary policy. Serious breaches of this policy, such as incidents of bullying or of social media activity causing damage to the organisation, may constitute gross misconduct and lead to dismissal.

Pupils, staff and volunteers must be aware of what is considered to be 'criminal' when using social media/Facebook or the internet and electronic communication in general.

While the list below is not exhaustive, it is provides some guidance in assessing the seriousness of incidents as well as determining appropriate actions.

All incident types below are considered criminal in nature but incidents would be subject to a full investigation in order to determine whether a crime has been committed or not**.**

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source.
- Misuse of logins (using someone else's login).
- Distributing, printing or viewing information on the following:
- Soft-core pornography.
- Hate material.
- Drugs.
- Weapons.
- Violence.
- Racism.
- Distributing viruses.
- Hacking sites.
- Gambling.
- Accessing age restricted material.
- Bullying of anyone.
- Viewing, production, distribution and possession of indecent images of children.
- Grooming and harassment of a child or young person.
- Viewing, production, distribution and possession of extreme pornographic images.

- Buying or selling stolen goods.
- Inciting religious hatred and acts of terrorism.
- Downloading multimedia (music and films) that has copyright attached. (Although this is illegal most police forces would treat this as a lower priority than the cases above).

Responding to misuse/incidents

Facebook (for incidents of cyberbullying or inappropriate behaviour)

If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed.

Failing that, having kept a copy of the page or message in question, delete the content and take action as appropriate.

For messages, the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.

For whole pages, the 'unfriend and report / block user facilities' are at the bottom of the left hand column.

Always try to cite which of the Facebook terms and conditions have been violated (see note 10 for the most likely ones) at http://www.facebook.com/terms.php or community standards at http://www.facebook.com/communitystandards/.

Note that Facebook are more alert to US law than UK. The process should be anonymous.

If the page is authored by someone under 13 then click on the following link: http://www.facebook.com/help/contact.php?show_form=underage .

To remove a post from a profile, hover over it and on the right there will be a cross to delete it.

To report abuse or harassment, email abuse@facebook.com. Facebook will acknowledge receipt of your email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint.

If all else fails, support the victim, if they wish, to click the 'Click CEOP' button http://www.thinkuknow.co.uk/ .

If the victim is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be undertaken via https://ssl.facebook.com/help/contact.php?show_form=delete_account.

They should be made aware of the privacy issues that might have given rise to their problem in the first place:

You will not bully, intimidate, or harass any user (1.3.6).

You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission (4.1).

You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law (5.1).

The school policies and protocols on child protection, safeguarding and e-safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity:

Child sexual abuse images.

Adult material which potentially breaches the Obscene Publications Act.

Criminally racist material.

Other criminal conduct, activity or materials.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way or are deemed as being inappropriate will *always* be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social networking sites, this will be addressed by the school in the first instance. If appropriate, disciplinary action will result. However, where necessary, the police will be involved and/or legal action pursued. The current Criminal Prosecution Service (CPS) guidance *'Guidelines on prosecuting cases involving communications sent via social media'* came into effect on 20 June 2013 and set out the approach that prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of a communication via social media. These guidelines are helpful when used alongside school employment and disciplinary policies in cases where staff misuse may the issue.

Monitoring and evaluation

The policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the governors' rolling programme of reviews.

Next school review due: July 2019