SOCIAL MEDIA GUIDELINES

1. Purpose

1.1 These guidelines outline the acceptable use of social media such as Twitter, Facebook, YouTube, LinkedIn and so on. Social media also covers blogs, published comments on websites in addition to video and image sharing websites such as Instagram and Snapchat.

1.2 These guidelines exist to assist employees by providing clear information about the acceptable use of social media and to safeguard all children.

2. Privacy settings

2.1 Information posted on personal social media profiles can make employees identifiable to students, parents, colleagues and contractors, as well as people they know in a private capacity. Employees should carefully consider the information they wish to make public when setting up an online profile particularly in relation to use of a photograph, details of their occupation, employer and work.

2.2 Employees are encouraged to review their access and privacy settings regularly for social media sites to control, restrict and guard against those who can access information and are advised to set privacy settings to the highest possible level.

3. Standards of conduct

3.1 Employees should be aware that they may be accountable for their actions on social media, including those outside of work, if these actions adversely affect the position for which they are employed.

3.2 Employees must not accept any current student of any age, or any ex-student under the age of 18 as a friend, follower, subscriber or similar on any personal social media account if the individual is only known to them in the capacity of a student in the course of their employment.

3.3 Any communication received from any current student of any age or any ex-student under the age of 18 on any personal social media sites must be reported to the Designated Safeguarding Lead at the earliest opportunity and in any event within 2 working days. This is necessary to safeguard all parties.

3.4 Communications through social media must not:

Bring the School or Trust into disrepute. For example by:

- Criticising or arguing with colleagues;
- Making offensive or defamatory comments;
- Posting images or links which are inappropriate, illegal, discriminatory or could be considered offensive
- Using derogatory or intimidating language

Breach confidentiality. For example by:

- Disclosing privileged, sensitive, personal or confidential information.

Impact on the implied term of trust and confidence. For example by:

- Engaging in activity which is incompatible with the employee's position
- Making comments which are bullying, harassing or discriminatory,
- Making derogatory comments on matters relating to their job or employment.
- Using social media to intimidate another individual
- Making comments in contravention of the organisation's policies, for example the Code of Conduct or Equality and Diversity policy.

The above examples are not an exhaustive list, but are indicative of types of misuse of social media.

4. Addressing allegations of misuse

4.1 All employees are required to adhere to this policy. Comments made through social media may constitute an act of misconduct and potentially gross misconduct, if the comments contravene any of the Trust or School policies, impact on or compromise the employee's ability to undertake their role,

4.2 Information available on social media sites could be produced as evidence, should it be necessary, either as part of any investigation.

4.3 Employees should take action if they find themselves the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others. If these issues are work related you should inform your Headteacher as soon as possible.

5. Action on leaving employment

5.1 Employees should update their profiles when leaving to remove reference, where it exists, to current employment at the School / The Two Counties Trust.

6. General Data Protection Regulation

6.1 All data within this policy will be processed in line with the requirements and protections set out in the General Data Protection Regulation.

Document management

Review cycle:	Every 3 years
Next review due:	July 2020
Policy owner	Head of Human Resources
Approving body:	Board of Trustees
Equality Analysis completed:	1.8.2017