

Online Safety Policy

**Our Mission Statement**

**We come together as Saint Mary’s family,**

**To learn, share our faith, and do our best to follow in the footsteps of Jesus**

**MODEL POLICY ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA**

The Governing Body of St. Mary’s Primary School Chipping adopted this policy on September 2018. The policy will be reviewed on an annual basis.

This Policy has been developed in consultation with the recognised Trade Unions and professional Associations.

* **PURPOSE**

This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

* **APPLICATION**

This Policy applies to all staff employed in delegated schools and those Teachers employed in Centrally Managed Services.

* **BACKGROUND**
* The use of social networking sites such as Facebook, Twitter, Pintrest, LinkedIn and MySpace has over recent years become the primary form of communication between friends and family. In addition there are many other sites which allow people to publish their own pictures, text and videos such as YouTube, Instagram and Snapchat.
* It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. For example many schools now use sites such as Facebook and Twitter as a means to enhance parental engagement.
* It is now widely acknowledged that use of such sites does not provide a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.
* Difficulties arise when staff utilise these sites and they do not have the relevant knowledge or skills to ensure adequate security and privacy settings. In addition there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.
* **GUIDANCE AND ADVICE**
* Employees who choose to make use of social networking site/media should be advised as follows:-
* That they should not access these sites for personal use during working hours;
* That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;
* That they do not conduct or portray themselves in a manner which may:-
* bring the school into disrepute;
* lead to valid parental complaints;
* be deemed as derogatory towards the school and/or it's employees;
* be deemed as derogatory towards pupils and/or parents and carers;
* bring into question their appropriateness to work with children and young people.
* That they do not form on-line 'friendships' or enter into communication with \*parents/carers and pupils as this could lead to professional relationships being compromised.
* On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.
* That they could face legal proceedings if comments they post about named individuals are found to have harmed their reputation.

(\*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to this Policy and as such they are potentially placing themselves at risk of formal action being taken under the school's Disciplinary Procedure.)

4.2 Schools should not access social networking sites in order to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination if for example the selection panel were to discover a candidate held a protective characteristic as defined by the Equality Act.

**5. SAFEGUARDING ISSUES**

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for those Working with Children and Young people in Education Settings (October 2015) states:-

|  |  |
| --- | --- |
| **12. Communication with Pupils (including the Use of Technology)**  In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. E-safety risks are posed more by behaviours and values than the technology itself.  Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.  Communication with children both in the ‘real’ world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand held devices. (Given the ever changing world of technology it should be noted that this list gives examples only and is not exhaustive.)  Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and  transparent and avoid any communication which could be interpreted as ‘grooming behaviour’  Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable.  Staff should, in any communication with children, also follow the guidance in section 7 ‘Standards of Behaviour’.  Staff should adhere to their establishment’s policies, including those with regard to communication with parents and carers and the information they share when using the internet. | This means that adults should:   * not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work * not give out their personal details * use only equipment and Internet services provided by the school or setting * follow their school / setting’s Acceptable Use policy * ensure that their use of technologies could not bring their employer into disrepute |

* **RECOMMENDATIONS**
* That this policy document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.
* That appropriate links are made to this document with your school/services Acceptable Use Policy
* That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites
* That employees are informed that disciplinary action may be taken in relation to those members of staff who conduct themselves in a way which is contrary to the advice and guidance outlined in this Policy. If such conduct is deemed to amount to gross misconduct this may lead to dismissal.

Reviewed Annually