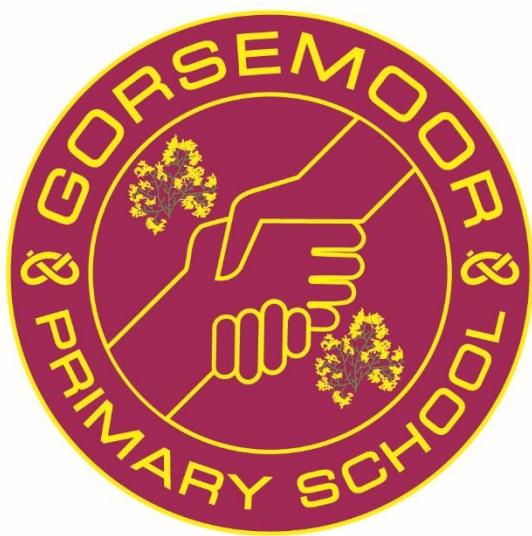


Social Networking and Cyber Bullying Policy



Date of Issue: April 2016

Review Date: April 2017

Approved by the Full Governing Body
on 15th June 2016

Audience: Staff/Governors/Public

Frequency of Review: Annually

Postholder responsible for Review: ICT co-ordinator

Recommended associated documents:

Computing Policy including Information Systems.

Online Safety Policy

Code of Practice for Employees in the use of Social Networking Sites and Electronic Media.

1.0 Protecting yourself and others in the use of Social Networking Sites and electronic media.

This code of practice provides employees with guidance to ensure they are taking necessary steps to protect themselves and others against Cyber bullying.

It also provides employees with practical guidance on how they can ensure that their conduct in relation to social networking sites and electronic media is in accordance with the code of conduct for all Local Government employees as interpreted by Staffordshire County Council in relation to social networking sites and electronic media.

2.0 Cyber Bullying

Definition: Cyber bullying is the use of Information and Communications Technology; particularly mobile phones and internet, deliberately to upset someone else.

(Cyber bullying: Guidance issued by the DCSF 2007)

Staffordshire County Council supports the view that cyber bullying represents a cruel, dangerous and inescapable form of bullying that causes humiliation, stress and trauma to its victims, and so believes that cyber bullying is not acceptable and will not be tolerated.

Staffordshire County Council is committed to the view that cyber bullying is never acceptable and is not tolerated.

3.0 Legislation

Although bullying is not a specific criminal offence, criminal law exists to prevent certain behaviours. These behaviours may constitute harassment, or cause fear of violence. Sending indecent, grossly offensive or threatening letters, electronic communications or other articles to another person is illegal.

Other legislation protects against the publication of obscene articles or data (e.g. over a school intranet), hacking into someone else's computer, invading their privacy, damaging their reputation or engaging in anti-social acts.

4.0 Protecting yourself against Cyber Bullying

There are simple measures that you can take to safeguard against cyber bullying.

- Being careful about personal information and images posted on the internet.
- Not leaving your mobile phone or personal computer around for others to gain access to or leaving details on view when left unattended.
- Choosing hard to guess passwords and not letting anyone know them
- Being aware of the risks of giving your mobile number or personal email address to others
- Making use of blocking facilities made available by website and service providers
- Not replying or retaliating to bullying messages
- Saving evidence of offending messages
- Making sure you inform others of any mobile phone or online bullying or harassment in accordance with relevant policies.

5.0 What action can you take?

You can report any incidents in relation to cyber bullying in the work environment in accordance with county council's Harassment and Bullying policy. If you make a complaint you have a right to have it investigated, and to seek assistance from managers, colleagues or trade unions in doing so.

Cyber bullying complaints will be investigated to obtain any evidence available and you can support this process by:

- Logging any incidents
- Noting the dates, times and content of messages and, where possible, the sender's identity or web address.

- Taking an accurate copy of the whole web page address, for example, helps service providers locate offending material. Such evidence may be required also to show to those who need to know, including police. Saving evidence of texts and images on the device can be useful. It is important they are not deleted.

In the non-work environment it may be appropriate to report incidents of cyber bullying direct to an internet service provider or mobile phone company. Content may be blocked and / or removed if it is illegal or breaks providers own terms and conditions. Some providers issue conduct warnings to users and are able to delete the accounts of those who have broken the rules.

Some cases may raise allegations against staff and in such cases, immediate referral should be made via the First Response Team to one of the Local Authority Designated Officers who will provide initial advice and guidance.

6.0 Code of Conduct

As a Condition of Service, all employees are expected to maintain conduct of the highest standard such that public confidence in their integrity is maintained.

This employment obligation is also reinforced, in relation to certain posts, by a duty to comply with external standards - as applies, for example, to Social Workers under the GSCC Codes of Conduct, or the requirements of professional bodies such as the Law Society.

You are reminded that care should be taken with the use of personal social networking sites to ensure the integrity of the county council is maintained and to this end you should ensure that you take account of the expectations of all employees with regard to all aspects of the employees code of conduct when posting information, messages, pictures or video footage these may include.

1. Bringing the county council into disrepute
2. Confidentiality
3. Policy restrictions

Care should be taken of the legislative measures that already exist e.g. Invasion of privacy, harassment.

7.0 Safeguarding

In order to safeguard yourself and potentially vulnerable adults and young people who you may work with you should ensure that your behaviour with regard to social networking sites is consistent with the standards of behaviour expected in normal day to day interactions with vulnerable adults and young people.

Communication that is undertaken via social networking sites is comparable to 'one to one' interaction in other contexts and individuals should avoid any activity which would lead any reasonable person to question their motivation and intentions.

You are reminded that it is expected that you:

- a) Always act in such a way as to promote and safeguard the wellbeing and interests of service users and colleagues.
- b) Take all reasonable steps to ensure the relationships with service users and colleagues are such that there can be no suggestion of impropriety whether by word or action
- c) Develop a friendly relationship between employee and service users, with clear boundaries. It is deemed an abuse of that professional relationship for an employee:
 - To enter into an improper relationship with a service user
 - To show favour towards a particular service user
 - To act in a threatening or aggressive manner or to use foul, abusive or profane language
 - To endeavour to exert an undue influence with regard to personal attitudes, opinions or behaviour which is in no way connected to the work of the Service.
- d) Take all reasonable steps to ensure no action or omission on your part or within your sphere of influence is detrimental to the condition or safety of service users

In order to preserve these standards of behaviour it is recommended that you decline any request from an existing or previous service user to be a 'friend' on your social networking site. Parents of children at school should not be 'friends' on your social networking site.

It is inappropriate to request contact with an existing or previous user of the service via this medium or any other form of electronic medium.

It is acknowledged that you may accept a service user as a 'friend' unintentionally and where this occurs you are advised to ensure that you remove this access as soon as you become aware of their status. You should do this in a way that does not jeopardise your professional relationship and should inform you Line Manager, if any significant conversation or activity occurs.

All employees are advised to ensure that when setting up social networking sites they should make full use of the range of tools which enable access to personal information to be restricted.