# Staff E-Safety Policy

This policy should be read in conjunction with the 'Computer Use Agreement'.

**This E-Safety policy covers the use of social networking and mobile phone applications by School Employees (staff). It will be distributed to all staff after Governor approval.**

**Cyber-bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.**

## Why do we need this policy?

The widespread availability and use of social networking applications bring opportunities to understand; engage and communicate with our audiences in new and exciting 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 duties to our School Community and partners, our legal responsibilities and our reputation.

Staff in schools, as well as children and young people, may become targets of cyber-bullying. Improvements in technology have led to improved communication and instant access to information. However, this technology can be abused and leave teachers vulnerable to harassment from students which they have no control over. Harassment can take place in a number of forms:

- Text messages.
- Picture/video-clips via mobile phone cameras.
- Mobile phone calls − silent or abusive messages; or stealing the victim's phone and using it to harass others.
- Emails − often sent using a pseudonym or somebody else's name.
- Harassment via social networking websites.

## Social Networking

Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications. Examples include Twitter, Facebook, MSN, You Tube.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

Any inappropriate communication received by school staff from students must be immediately reported to the Head Teacher and Designated Child Protection Officer and procedures for safeguarding followed.

If a member of staff is made aware of any other inappropriate communications involving any child and social networking these must be reported immediately as above.

**The school 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 these Terms of Use. All School representatives 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, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School Equality and Safeguarding Policies.**

## Mobile Phones

Staff should take good care of their mobile phones. They should secure their phones when not in use, using the phone's security code.

If it is absolutely necessary for an employee to lend a student a mobile phone, staff should use a school mobile rather than one owned by an individual employee. If this is not possible, the staff member should supervise the call and delete any numbers used afterwards. If being able to contact students by their mobile becomes necessary – for example on a school trip – school employees should use school-owned mobiles wherever possible to store numbers and contact students. Numbers can be deleted following the event, and learners will not have access to an employee's personal number.

**What can you do to protect yourself from being harassed by students?**

**Keep your security settings on social networking websites at the highest level.**
**DON'T give out personal email addresses or telephone numbers to students.**
**DON'T telephone a student at home on your mobile phone.**
**Exercise your power to confiscate mobile phones if you believe they have been used inappropriately.**

## The Internet

Many school employees use the web and social networking services such as Facebook, Flickr, and Ning for work-related projects or for personal use. While school employees are private individuals, they also have professional reputations and careers to maintain. Additionally, employees are required not to do anything to endanger the health and safety of their colleagues or others.

Staff are strongly advised in their own interests to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff also need to be aware that many employers and other agencies now carry out web and social network service searches to find online information about staff – background, interests, career experiences and self-presentation. All staff, perhaps especially new staff in training and induction need to be advised to ensure that information available publicly about them is accurate and appropriate.

Privacy on the internet seldom means communications are entirely private, even messaging. Think of internet communications as equivalent to sending postcards. Information sent using official school accounts or equipment will usually be accessible for monitoring purposes (this will be outlined in the school's Acceptable Use Policy) and may be requested under the Data Protection Act. Managing personal information effectively makes it far less likely that information will be misused.

**When publishing information about yourself or having conversations with others online, it is important to be mindful of how you present yourself, who can see your content, and how you can manage this appropriately.**

**When publishing information, personal contact details, video or images, ask yourself if you would feel comfortable about a current or prospective employer, colleague, student or parent, viewing your content.**

**Make sure you understand who is allowed to view your content on the sites that you use – and how to restrict access to your account where necessary. If you are not clear about how to restrict access to your content to certain groups of people, regard all of your content as publicly available and act accordingly.**

**You can also check to see that other people aren't misrepresenting you or treating you unfairly online. If you find things you object to, you can ask the poster to take these down in the first instance. Where cases are work related, these should be reported to your line manager or to the appropriate person as soon as possible. More serious incidents, including cyber-bullying, will require a formal response from your employer, and will be dealt with within the school's disciplinary frameworks, or in more serious cases, legal frameworks.**

## You can check to see if others are creating or posting objectionable material about you online

Use search engines to check what images and text are associated with your name, or with your school and your name. This will help establish what information other people can easily find about you.

Use search facilities within specific social networking sites – some may require you to be a logged in member.

Staff often become aware of other people posting objectionable material about them from other learners. Encouraging everyone to report any incidents they find, rather than being a passive bystander, is an important strand of cyber-bullying prevention. 'Friending' refers to the act of giving contacts permission to view information or contact you within web-based services.

The terminology will vary from service to service – 'Friends' may be called contacts or connections, for example. Most social sites enable you to give different levels of access and set privacy levels on your own content and activity. These functions will vary from service to service but typically include:

- Information that is only available to the account holder
- Information that is accessible by contacts on the account holder's approved list, and
- Information that is made publicly available, either within the service or across the whole of the internet. 'Friends' does not necessarily refer in this case to people who are your

actual friends, although you may choose to restrict your connections to that. 'Friends' in this context may also be work colleagues, family members, and people that you have met online. If you have a social networking account, do not friend students or add them to your contact lists. You may be giving them access to personal information and allowing them to contact you inappropriately. They may also be giving you access to their personal information and activities.

- Don't use web-based social networking sites for a class, instead ask students to create new, work-focused files for themselves within the school's shared intranet.

## What to do if you receive abusive communications

Report the incident, at the earliest opportunity, to your Line Manager, or a member of SLT and seek support. Staff should never retaliate to, i.e. personally engage with, cyber-bullying incidents.

Keep any records of the abuse – text, emails, voice mail, web site or instant message. Do not delete texts or emails. Take screen prints of messages or web pages, and be careful to record the time, date and address of the site.

Where the perpetrator is known to be a current student or co-worker, the majority of cases will be dealt with most effectively by the school's own mediation and disciplinary procedures.

Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated. However, it is important to be aware that this may not necessarily lead to an identifiable individual. For instance, if another person's phone or school network account has been used, locating where the information was originally sent from will not, by itself, determine who the bully is. There have been cases of people using another individual's phone or hacking into their IM or school email account to send harmful messages.

If a potential criminal offence has been committed and the school is not able to identify the perpetrator, the police may issue a RIPA (Regulation of Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message.

A member of SLT should contact the police where it appears that a law has been broken – for example, where death threats, assault, or other racially motivated criminal offences are involved. Where a potential criminal offence has been identified, the school should ensure that any internal investigation does not interfere with police inquiries. School staff are of course able to report incidents directly to the police.

There have been cyber-bullying incidents where students have made unfounded, malicious claims against staff members. It is of course critical to take every claim seriously and investigate it thoroughly. In cases where an allegation is made that an employee or volunteer has: behaved in away that has harmed or may have harmed a child; possibly committed a criminal offence against or related to a child; or behaved towards a child or children in a way that indicates s/he is unsuitable to work with children; then that allegation should be reported

to the Head Teacher immediately. The Head Teacher will then decide whether to consult the police or children's social care colleagues.

Where online content is upsetting and inappropriate, and the person or people responsible for posting is known, the quickest way to get material taken down is likely to be to ensure that the person who posted it understands why the material is unacceptable and to request that they remove it.

**If the person responsible has not been identified, or will not take material down, the school leadership team member will need to contact the host (for example, the social networking site) to make a report to get the content taken down. The material posted may breach the service provider's terms and conditions of use and can then be removed.**

In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the victim will need to establish their identity and lodge a complaint directly with the service provider. Some services will not accept complaints lodged by a third party. In cases of a mobile phone abuse, for example, where the person being bullied is receiving malicious calls or messages, the account holder will need to contact their provider directly.

Before a school or individual contacts a service provider, it's important to be clear about where the content is – for example by taking a screen capture of the material that includes the URL or web address. If you are requesting they take down material that is not illegal, be clear how it contravenes the site's terms and conditions.
In cases of actual/suspected illegal content, the school's designated representative should contact the police. The police will be able to determine what content is needed for evidential purposes.

**Keep passwords secret and protect access to your accounts.**

**Don't friend students on personal social networking services.**

**Keep personal phone numbers private and don't use personal mobiles to contact students or parents.**

**Keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, and keep phones secure while on school premises.**

**Don't post information about yourself publicly that you wouldn't want employers, colleagues, students or parents to see.**

**Ensure that rules regarding the use of technologies are consistently enforced.**

**Don't personally retaliate to any incident.**

**Report any incident to the appropriate member of staff in a timely manner.**

**Keep any evidence of an incident.**

## User Areas

Members of staff should be aware that no other person can use the computer when it is logged into their user area on the network. This applies to students and other members of staff. It is an offence in legal terms to use a computer that it logged into someone else's user area of the network.