# E-SAFETY: PROTECTING SCHOOL STAFF
## *NUT Guidance and Model Policy*

**PROTECTING SCHOOL STAFF**

E-Safety is a key issue for all schools. Staff in schools, as well as pupils, may become targets of cyberbullying. Cyberbullying takes place when an individual or group of people use technology such as the internet, mobile phones, e-mail, chat rooms, or social networking sites to bully, threaten or embarrass their victim.

Cyberbullying is best dealt with within a robust framework of policy and practice, which includes and supports the whole-school community. The NUT believes, therefore, that every school should have a policy on e-safety, which should cross-refer to other policies dealing with bullying/harassment. Supplementing this guidance, at Appendix 1, is a model policy which governing bodies should be invited to adopt, where an equivalent policy is not already in place.

These are also workload issues associated with technology in schools.

Time to read and respond to e-mails should be incorporated into a teacher's directed time budget, as part of their other professional duties. Teachers should not be expected to deal with their e-mail correspondence in the evenings or at weekends. There should also be no expectation on the part of management, pupils or parents, that instant replies will be sent.

The NUT believes that every school should ensure that:

- school governors, head teachers, and senior management team members are familiar with the Government's **Safe to Learn Cyberbullying** Guidance. This can be found online at www.digizen.org/cyberbullying and at www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying

- the whole-school community should understand what is meant by `cyberbullying', its potential impact, how it differs from other forms of bullying and why it is unacceptable.

- all staff should be provided with information and professional development opportunities regarding understanding, preventing and responding to cyberbullying. It is particularly important that they understand the child protection and other legal issues that may relate to cyberbullying incidents.

- school policy, guidance and information relevant to cyberbullying is regularly reviewed, to ensure that it meets the needs of pupils and staff. These are likely to include: behaviour policies and policies governing the use of mobile phones and camera mobile phones in schools.

- the reporting routes and relevant responsibilities are made clear. A nominated member of the senior management team should lead on, and oversee, anti-cyberbullying activity and incidents. Some staff may find it difficult to report instances of cyberbullying to the nominated member of staff, and where this is the case they should feel free to seek advice from their NUT school representative.

- the benefits of technology are understood and promoted, whilst at the same time recognising that there are dangers which must be addressed.

- the impact of prevention and response policies and practice is monitored annually. Staff, pupils and parents should feel confident that their school effectively supports those who are cyberbullied.

**School employees should expect that:**

- all incidents that they report will be recorded.

- the school will respond to an incident in a timely and appropriate manner, or support the member of staff concerned to do so.

- appropriate personal support, or information enabling them to access appropriate personal support will be provided.

- information on the safe use of the school's communications network will be provided to them.

- the school will approach third party agencies on their behalf in order to request that inappropriate material is removed, where possible.

- the school will support the staff member in cases where it is necessary for the person being bullied to contact the service provider directly.

- where appropriate, the school will contact the police or external agencies.

If a teacher is not satisfied with the way in which a cyberbullying incident has been dealt with, he or she should seek advice from the NUT.

Appendix 1 to this document is an NUT model policy on e-safety. Appendix 2 sets out a list of do's and don'ts for school staff.

**Related NUT Guidance Documents available from www.teachers.org.uk**

Harassment and Bullying of Teachers: Guidance for Members, School Representatives and Health and Safety Representatives available from www.teachers.org.uk/node/12522

Pupil Behaviour – Advice, Guidance and Protection from the NUT available from www.teachers.org.uk/node/11054

Mobile Phone Photography – Health and Safety Issues available from www.teachers.org.uk/node/12497

**APPENDIX 1**

## NUT MODEL POLICY ON E-SAFETY

### Introduction

Staff in schools, as well as children and young people, may become targets of cyberbullying. Like other forms of bullying, cyberbullying can seriously impact on the health, well-being, and self-confidence of those targeted. It may have a significant impact not only on the person being bullied, but on their home and work life too. Career progression may be affected, and there have been cases where the person bullied has chosen to leave the education sector altogether. Dealing with incidents quickly and effectively is key to minimising harm in potentially highly stressful situations.

This employer/governing body_____ will ensure that comprehensive e-safety education is provided that includes support for both pupils and staff on managing personal information in on-line environments, and in using personal and social technologies responsibly.

### Roles and Responsibilities

This employer/governing body _____ (insert as appropriate) will ensure that this policy will be reviewed and monitored periodically.

The head teacher _____ will ensure that the school has a nominated person as e-safety lead (a member of the senior management team tasked with overseeing and managing the recording, investigation and resolution of cyberbullying incidents).

Teaching staff will familiarise themselves with this e-safety policy and procedures.

Staff e-mails that are marked ‘personal’ and/or ‘union business’ will not be read by school management without prior consent.

### Responding to incidents and reporting

- Staff should never personally engage with cyberbullying incidents. They should report incidents to the nominated person appropriately and seek support.

- Staff should keep any records of the abuse – text, e-mails, voice mail, web site or instant message. Screen prints of messages or web pages should be taken and time, date and address of site should be recorded.

- Staff should inform the nominated person of incidents at the earliest opportunity.

- Where the perpetrator is known to be a current pupil or colleague, the majority of cases will be dealt with most effectively under the relevant school disciplinary procedure.

- Monitoring and confiscation must be appropriate and proportionate. Except in exceptional circumstances (for example, where disclosure would prejudice the conduct of a criminal investigation) parents, employees and learners will be made aware, and their consent sought, in advance of any monitoring (for example, of e-mail or internet use) or the circumstances under which confiscation might take place.

- Where a potential criminal offence has been identified, and reported to the police, the school will ensure that any internal investigation does not interfere with police inquiries.

- Where pupils are found to have made unfounded, malicious claims against staff members, relevant and appropriate disciplinary processes will be applied with rigour, as is the case in relation to physical assaults.

- Staff should report all incidents to the nominated person. The nominated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

**Action by school: Inappropriate Use of Social Networking Sites**

Following a report of inappropriate use of social networking sites, the nominated person will take the following action:

- Where online content is upsetting and inappropriate, and the person or people responsible for posting are known, the nominated person will explain why the material is unacceptable and request that it be removed.

- If the person responsible has not been, or cannot be, identified, or will not take material down, the nominated person will contact the host (for example, the social networking site) with a view to removal of the content. 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 nominated person will support the victim in establishing their identity and lodging a complaint directly with the service provider. Some service providers will not accept complaints lodged by a third party. In cases of 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 the nominated person contacts a service provider, he or she will check the location of the material – for example by taking a screen capture of the material that includes the URL or web address. If the nominated person is requesting that the service provider takes down

material that is not illegal, he or she will be clear how it contravenes the site's terms and conditions.

**Where the bully is a member of the school community (including parents/carers) the school will:**

- deal with harassment and bullying under the relevant school procedure;
- take care to make an informed evaluation of the severity of the incident;
- deliver appropriate and consistent sanctions; and
- provide full support to the staff member(s) affected.

The employer/governing body _____ (insert as appropriate) recognises its legal duty to protect staff from unlawful harassment as well as mental and physical injury at work.

In cases of potentially criminal content, the nominated person will consider whether the police should be involved, following appropriate liaison with staff, and parents where necessary.

Useful information for the nominated e-safety lead including a list of service providers is attached.

## USEFUL INFORMATION FOR NOMINATED E-SAFETY LEADS

### Mobile Phones

All UK mobile phone operators have nuisance call centres set up and/or procedures in place to deal with such instances. They may be able to change the number of the person being bullied. Mobile operators cannot bar a particular number from contacting a phone, but some phone handsets do have this capacity. Action can be taken against the bully's phone account (e.g. blocking their account) only with police involvement.

**Contacts:**

**O2**: ncb@o2.com or 08705214000.

**Vodafone**: 191 from a Vodafone phone or 08700700191 for Pay Monthly customers and 08700776655 for Pay as you Go.

**3**: Call 333 from a 3 phone or 08707330333.

**Orange**: Call 450 on an Orange phone or 07973100450 for Pay as you Go, or 150 or 07973100150 for Pay Monthly.

**T-Mobile**: Call 150 on a T-Mobile phone or 08454125000.
A list of service providers is attached at Appendix 2.

**Virgin**: Call 789 from a Virgin phone or 0845 6504500.

### Social networking sites (e.g. Bebo, FaceBook, MySpace)

Contacts of some social network providers:

**Bebo**: Reports can be made by clicking on a `Report Abuse' link located below the user's profile (top left-hand corner of screen) on every Bebo profile page. Bebo users can also report specific media content (i.e. photos, videos, widgets) to the Bebo customer services team by clicking on a `Report Abuse' link located below the content they wish to report. www.bebo.com/Safety.jsp

**Facebook**: Reports can be made by clicking on the `Report' link located on pages throughout the site. Facebook users can also report another user by using the "Report/Block" link that appears at the bottom of a user's profile page or by listing the user's name in the "Block List" box that appears at the bottom of the Privacy page.

**MySpace**: Reports can be made by clicking on the `Contact MySpace' link at the bottom of every MySpace page and selecting the `Report Abuse' option. Alternatively, click on the `Report Abuse' link located at the bottom of each user profile page and other user-generated pages. Inappropriate images can be reported by clicking on the image and selecting the `Report this Image'

option. Additionally, school staff may emails MySpace directly at schoolcare@myspace.com www.myspace.com/safety

## Video and photo hosting sites

**YouTube**: Logged in YouTube members can report inappropriate content by using the `flat content as inappropriate' function which appears under every video. http://icanhaz.com/YouTubeAbuseSafety.

**Flickr**: Reports can be made via the `Report Abuse' link which appears at the bottom of each page. Logged in members can use the `flag this photo' link to report individual pictures. www.flickr.com/guidelines.gne

## Instant Messenger

It is good practice for Instant Messenger (IM) providers to have visible and easy-to-access reporting features on their services. Instant Messenger providers can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for the service provider is archived or recorded conversations, and most IM providers allow the user to record all messages.

**Contacts of some IM providers:**

**MSN**: When in Windows Live Messenger, clicking the `Help' tab will bring up a range of options, including `Report Abuse'.

**Yahoo!**: When in Yahoo! Messenger, clicking on the `Help' tab will bring up a range of options, including `Report Abuse'.

## Chatrooms, individual website owners/forums, message board hosts

It is good practice for chatroom providers to have a clear and prominent reporting mechanism to enable the user to contact the service provider. Users that abuse the service can have their account deleted. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use.

**APPENDIX 2**

## How to Stay 'Cybersafe' – Do's and Don'ts

Staff should:

- not post information and photos about themselves, or school-related matters, publicly that they wouldn't want employers, colleagues, pupils or parents to see;
- keep passwords secret and protect access to accounts;
- not befriend pupils or other members of the school community on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils and let school management know if they decide to do this.);
- keep personal phone numbers private and not use their own mobile phones to contact pupils or parents;
- use a school mobile phone when on a school trip;
- keep a record of their phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school premises and report thefts to the police and mobile operator as soon as possible;
- ensure that school rules regarding the use of technologies are consistently enforced;
- not personally retaliate to any incident;
- report any incident to the appropriate member of staff in a timely manner;
- keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material, including the URL or web address.
- use school e-mail address only for work purposes.
- be aware that if they access any personal web-based e-mail accounts via their school network, that these may be subject to the school's internet protocol which could include monitoring and surveillance.
- request assurances from management that any e-mails marked 'personal' and/or 'union business' will not be read without their prior consent.