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

PROTECTING SCHOOL STAFF

E-Safety is a key issue for all schools as it can pervade all aspects of school life. Staff in schools, as well as pupils, may become targets of cyberbullying. Cyberbullying is a whole school community issue. It 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. It is important that schools make it clear that bullying including cyberbullying of staff is unacceptable.

Though e-safety is not just confined to cyberbullying of course, 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.

Teachers need to be aware of their online reputation and have to recognise that comments that they make online can be seen by others particularly when using social networking sites. The UK Safer Internet Centre (www.saferinternet.org.uk/advice-and-resources) provides help for staff on how to stay safe on-line, as well as how to support young people in staying safe. It is funded by the European Union and provides a helpline for professionals who work with children and young people in the UK, specifically tackling e-safety. The helpline is available at helpline@saferinternet.org.um, tel 0844 381 4772. In relation to young people, help is available on safe use of social networking sites, cyber-bullying, 'sexting' and child protection issues. Teachers can also obtain advice about protecting their own on-line reputation. The helpline operates between 10 am and 4pm, Monday to Friday.

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. Senior management in particular need to recognise that any electronic communications they may send to teachers in the evening or at weekends will not necessarily be responded to until the next available working day. 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 **Let's Fight it Together – What we can all do to prevent cyber bullying** Guidance. This can be found online at https://www.education.gov.uk/publications/standard/publicationDetail/Page1/DCSF-00239-2008. Also see www.digizen.org/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 and other e-safety issues. It is particularly important that they understand the child protection and other legal issues that may relate to cyberbullying and e-safety incidents.

- school policy, guidance and information relevant to cyberbullying and e-safety 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 and/or smart phones and other portable devices including tablets in schools.

- the reporting routes and relevant responsibilities are made clear. A nominated member of the senior management team should lead on, and oversee, E-safety within the school including 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 – this should include guidance about how school devices issued to staff can and cannot be used both on and off the school premises.

- 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

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

Introduction

Staff in schools, as well as children and young people, may be affected by e-safety issues including 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. E-safety, however, is about more than cyberbullying. It is about protecting one's on-line reputation, the managing of personal information and the responsible use of technologies.

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 e-safety incidents).

All 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. Where appropriate, they should report incidents to the nominated person and/or seek support.

- Staff should keep any records of the abuse – text, e-mails, voice mail, web site or instant message. If appropriate, screen prints of messages or web pages could be taken and time, date and address of site should be recorded though care needs to be taken when copying certain images.

- 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. The NUT believes that the practice of searching the contents of pupils' phones is unlikely to be used other than rarely due to its impracticability and the damage it could do to teacher/pupil relationships. The NUT believes that schools will be best served by including clear statements within the school's behaviour policy about the situations in which this may be done, after consulting fully within the school community. Any teachers or other staff who are to be asked to undertake such searches, which the NUT believes will only be in exceptional circumstances, should be given full guidance and any necessary training. It is of utmost importance that individual school staff operate fully within the school's procedures. Searches without consent can only be carried out on the school premises or, if elsewhere, where the member of staff has lawful control or charge of the pupil, for example on school trips in England or in training settings. The powers only apply in England. (See NUT briefing note 'Screening and Searching for Prohibited Items' at http://www.teachers.org.uk/node/17402 for further information).

- 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. In cases of cyberbullying, 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 alleged 'offender' 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.

APPENDIX 1

USEFUL INFORMATION FOR NOMINATED E-SAFETY LEADS

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

Mobile phones

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. They can help you to change the number of the person being bullied if necessary. It is not always possible for operators to block particular numbers from contacting the person being bullied, but many phones, such as IPhones allow users to block phone numbers.

If you want to prosecute the individual contact the police. If a bully is making direct threats which you feel constitute a real danger, phone 999. If there isn't an immediate danger, then contact the non-emergency number 101. The mobile provider can work closely with the police and can usually trace malicious calls for them.

Contact details for service providers:

Service provider	From your mobile	Pay as you go	Pay monthly contracts
O2	202 (pay monthly) 4445 (pay as you go)	03448 090 222	03448 090 020
Vodaphone:	191	08700 776 655	08700 700 191
3	333	08707 330 333	08707 330 333
EE (Orange and T Mobile)	150	07953 966 250	07953 966 250
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Contact details for social networking sites:

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools. Advice can be found here http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/safety-tools-on-online-services

Facebook	YouTube
Read Facebook's rules	Read YouTube's rules
Report to Facebook	Report to YouTube
Facebook Safety Centre	YouTube Safety Centre

Instagram Read Instagram's rules Report to Instagram Instagram Safety Centre	**Twitter** Read Twitter's rules Reporting to Twitter
Vine Read Vine's rules Contacting Vine and reporting	**Kik Messenger** Read Kik's rules Reporting to Kik Kik Help Centre
Ask.fm Read Ask.fm's 'terms of service' Read Ask.fm's safety tips **Reporting on Ask.fm:** You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.	**Tumblr** Read Tumblr's rules Report to Tumblr by email If you email Tumblr take a screen shot as evidence and attach it to your email

Video and photo hosting sites

YouTube: Logged in YouTube members can report inappropriate content at:
http://support.google.com/youtube/bin/answer.py?hl=en&answer=95403

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 details for 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'.

WhatsApp: There are details in the FAQs section on blocking other users (http://www.whatsapp.com/faq/en/general/21242423). There isn't a service to report abuse, but details can be emailed to support@whatsapp.com

Snap Chat: safety information and reporting options are available at - https://support.snapchat.com/ca/abuse

Skype: https://support.skype.com/en/faq/FA10001/how-do-i-report-abuse-by-someone-in-skype

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

Do

- be aware of your on-line reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available on-line information. Remember, the internet never forgets!;
- keep passwords secret and protect access to accounts – always log off from any device that you have been using, even if you are only stepping out of the room for a moment and ensure that all phones and tablet devices are secured with a passcode;
- regularly review your privacy settings;
- discuss expectations with friends – are you happy to be tagged in photos?;
- be aware that, increasingly, individuals are being held to account in the courts for the things they say on social networking sites;
- keep personal phone numbers private and don't use your own mobile phones to contact pupils or parents;
- use a school mobile phone when on a school trip;
- keep a record of your 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 (Note: you can find out your IMEI number by typing *#06# on your handset – the number will be displayed on the screen);
- ensure that school rules regarding the use of technologies are consistently enforced;
- 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 (staff need to be aware that taking a screenshot of content which is potentially illegal could result in staff committing a criminal offence) including the URL or web address.
- use school e-mail address only for work purposes.
- be aware that if you access any personal web-based e-mail accounts via the 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 your prior consent.

- raise genuine concerns about your school or certain members of staff using your employer's whistle blowing or grievance procedure.

Don't

- post information and photos about yourself, or school-related matters, publicly that you wouldn't want employers, colleagues, pupils or parents to see;

- befriend pupils or other members of the school community on social networking sites. (You should consider carefully the implications of befriending parents or ex-pupils and let school management know if you decide to do this.);

- personally retaliate to any incident, bullying messages;

- criticise your school, pupils or pupils' parents online.

More helpful tips are available from the UK Safer Internet Centre at www.saferinternet.org.uk under 'Advice and Resources'.