School Human Resources Advice Team
Human Resources & Development.

E-Safety Model Policy

This procedure has been agreed by the following Professional Associations / Trade Unions representing staff in schools:-

- National Union of Teachers
- National Association of Schoolmasters Union of Women Teachers
- Association of Teachers and Lecturers
- National Association of Head Teachers
- Association of School and College Leaders
- UNISON
- GMB

Contents

1. Introduction

E-safety is becoming an increasingly powerful tool for schools that should be utilised in teaching and learning. However, e-safety is also the responsibility of all staff in school. It is particularly important therefore that staff are provided with information to increase their understanding of e-safety issues to help prevent any breaches that will ensure that staff and pupils are kept safe in school. This may include for example 'cyber bullying' which takes place when an individual or group of people use technology such as the internet, mobile phones, email, chat rooms or social networking sites to bully, threaten or embarrass their victim.

Social networking activities conducted online outside work, such as blogging, involvement in social networking sites such as Facebook, MySpace or Twitter and posting material, images or comments on sites such as You Tube can have a negative effect on a school's reputation **or an individual's reputation**. Such activities may also contravene a school's commitment to safeguarding children.

This policy has been written in conjunction with other LA e-safety advice available on the Learning Gateway to help raise awareness of e-safety issues for school staff. It also sets out the key principles and code of conduct that is expect from staff working in Shropshire schools with regard to their responsibilities with e-safety.

This Policy has been approved by Shropshire Council for the adoption by Shropshire schools, including maintained schools, Voluntary Controlled, voluntary Aided and Academies.

This policy will apply to all teaching and non-teaching staff, whether full-time or part-time, employed in Shropshire schools. This policy also applies to governors, friends and volunteers working in Shropshire schools. It is not intended to apply directly to pupils and parents although section 2.7 provides further links to LA e-safety advice on the Learning Gateway and other publications that support raising awareness of e-safety issues for the whole school community. The LG e-safety guidance should be read in conjunction with this policy to ensure schools meet their e-safety obligations including Ofsted requirements

This policy takes account of employment legislation and best practice guidelines in relation to e-safety in addition to the legal obligations of governing bodies and the relevant legislation. This includes:

- Data Protection Acts 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Freedom of information Act 200
- Human Rights Act 1998
- Regulation of Investigatory powers Act 2000

2. Policy

Name of school

……

Date agreed by Governing Body

……

Date for Review

……

2.1. Purpose

This policy sets out this School's policy on e-safety issues both inside and outside of work. The objectives of this policy are to:

- Set out the key principles and code of conduct expected of staff in this school in respect of e-safety so that pupils and staff are safe guarded.
- Ensure that colleagues and members of this school are treated with professionalism and respect.
- Ensure that everyone at this school is protected from any malicious cyber bullying and misinterpretations which can arise from the misuse of e-safety.
- Ensure that staff and the whole school community know where to access further information about e-safety.
- Ensure that that staff feel able to report any concerns about breaches of e-safety to a nominated person for e-safety (where this is not their line manager or head teacher.)
- Ensure that staff understand their responsibility to also protect themselves and the reputation of the school by using social networking sites responsibly outside of work.

School staff have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils, and public in general and all those in the whole school community. Safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

The guidance contained in this policy identifies the behaviours that are expected of schools' staff who work with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

2.2. E-Safety Code of Conduct

Under the schools E-Safety Code of Conduct, everyone at this school must ensure that they:

- Communicate with pupils and staff in an open and transparent way using the school phone number and email address. (Personal e-mail addresses should never be given to pupils or parents.)

- Keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents in a professional capacity. (There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle, or where staff are transport escorts or where for PTA

purposes for example both staff and parents have exchanged personal numbers). These contacts however, will be easily recognised and openly acknowledged. Staff have a responsibility to make sure that any such contact known to the senior leadership team.)

- Keep their mobile phone secure whilst on school premises. All mobile phones should be switched off whilst staff are on duty unless there are good reasons that have been confirmed with a member of the senior leadership team.

- Never 'friend' a pupil at the school where they are working onto their social networking site.

- Never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil.

- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments to anyone or about anyone in the whole school community or about the school.

- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings (this should include past postings.)

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about them which may compromise their personal safety and security.

- Should not share their work log-ins or passwords with other people.

- Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

The following are **not considered acceptable** at this school:

- Under no circumstances should staff make reference to any staff member, pupil, and parent or school activity/event during their social use of the internet and other communication technologies.

- The use of the school's name, logo, or any other published material without written prior permission from the Head teacher. This applies to any published material including the internet or written documentation.

- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

2.3 Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the School's Disciplinary Procedure and it is possible that this may be considered to constitute Gross Misconduct and could therefore lead to dismissal.

- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Head teacher of the justification for any such action already taken or proposed. The Head teacher will in turn seek advice from Shropshire Council where appropriate.

2.4 Cyber bullying

Cyber bullying is defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

It is important for all staff to understand the issues related to cyber bullying given that they as well as pupils may become targets. Section 2.7 provides a sign post for further information for the whole school community on this subject which includes further information for staff to help detect and prevent pupil cyber bullying.

Prevention activities are key to ensuring that staff are protected from the potential threat of cyber bullying. Staff should have access to this policy and any other related policies, or information that covers their responsibilities with regards to e-safety behaviour and communication.

If a member of staff considers that cyber bullying has taken place, they should:

- keep records of the abuse, text, e-mails, website or instant message

- Not delete texts or e-mails.

- Take screen prints of messages or web pages and be careful to record the time, date and place of the site.

- Report all incidents of cyber bullying to their line manager or the Head teacher or the nominated member of the senior management team (SMT) who leads on and oversees anti-cyperbullying activities.

Staff can expect that their line manager, head teacher or nominated member senior responsibility for e-safety will:

- Take reported incidents seriously and record them
- Respond to staff in a timely and appropriate manner
- Provide appropriate support or enable appropriate support to be accessed
- Support the member of staff to approach the person or the Server provider directly as in the case of mobile phone abuse case this may only be achievable by the account holder as third party complaints may not be accepted)
- Where appropriate and in agreement of the wishes of the person who has reported the incident, report the actions to the police.

If the alleged perpetrator is the head teacher then incidents should be reported to the Chair of Governors.

Action by the School

Following a report by the line manager, head or nominated person for e-safety the following action may be necessary:

- Explain to the known perpetrator that the content is unacceptable and request that it be removed.
- Where the perpetrator is known to be a current colleague, the case is likely to be dealt with effectively under the Schools Disciplinary Procedure. Head teachers should contact their nominated HR Officer for advice and support as necessary.
- Where a potential criminal offence has been identified by a current colleague (and reported to the police and the LA), the Head will ensure that any internal investigation is held until the police investigation is complete.
- Where the perpetrator is known to be a current pupil, the case is likely to be dealt with by the Head teacher under the relevant pupil behaviour procedure.
- Where the perpetrator is known to be a member of the school community (including/ carers and parents) the Head teacher will ensure that an informed evaluation of the incident is made with liaison with the member of staff and the parent (including appropriate police involvement).
- Monitoring and confiscation must be appropriate and proportionate except where disclosure would prejudice the conduct of a criminal investigation. Any monitoring of pupil or staff email or internet use as a result of a cyber bullying complaint must not take place without prior consent obtained from the parent or member of staff.

If the person has not or cannot be identified or refuses to remove the material the head, line manager or nominated person for e-safety will contact the host with the view to remove the material. (It will be necessary to firstly check the location of the material that includes URL or web address so that if the material is not illegal, it will be clear how it contravenes the site's terms and conditions.)

2.5 Safer Online Behaviour

Some social networking sites and other web-based sites have fields in the user profile for job title etc. School staff should carefully consider the information they input on the site as it may identify their profession or the school where they work. In some circumstances this could damage the reputation of the school, the profession or the local authority.

In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Shropshire Council could result in formal action being taken against them. This includes the uploading of photographs which might put the school into disrepute.

2.6 Access to Inappropriate Images and Internet Usage

There are extremely limited circumstances that will justify staff possessing indecent images of children and these circumstances are likely to be limited to situations when staff are reporting incidents or participating in investigations. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children are illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Where indecent images of children are found by staff, the police should be immediately informed. Schools should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, Shropshire Council Schools HR Advice Team should be informed

and advice sought. The school should not attempt to investigate or evaluate the material themselves until such advice is received.

2.7 Links to Internal and External E-Safety Information & Other School Policies

Other School Policies

This policy should also be read in conjunction with the following school policies:

- Schools' Information and ICT Security Policy (year)
- Child Protection Policy
- Schools staff Professional Code of Conduct
- Schools Disciplinary Procedure
- Schools Harassment & Bullying Procedure
- Equality Plan
- The Schools Induction procedures

Learning Gateway

The Learning Gateway includes comprehensive e-safety information for schools staff, parents and students much of which has been based on the guidance from the 360 degree national framework from the South west grid for learning (SWGL). The documents have then been approved through the SSCB e-safety sub group and headteachers' ICT/e-learning group.

From the front Shropshire Learning Gateway page, go to the e-safety tab at the top. This then includes links drop downs for Parents, Staff and Students:

Staff –includes tips on how to evaluate the behaviour and safety of pupils at the school using guidance from the Ofsted Behaviour and Safety schedule.

- e-safety & Ofsted
- Resources & links
- Policies & Acceptable Use Policies (AUP's) including :

  -Social Media Use } a starting point for schools to adapt
  -e-safety policy example} a starting point for schools to adapt
  -360 degree safe advice – sheds light on what should be in an e-safety policy
  - e-safety policy guidance
  - safe guarding children becta checklist
  -guidance for safer working practice for adults who work with children & young people
  -cyber bullying- support for school staff
  -Acceptable Use Policies (wmnet recommended versions)
  -Byron Report-school self evaluation, a response to the Byron Review
  -Byron Report
- NQTs
- Safer Internet Day
- 360 Degree Safe
- Support

Parents –includes tips for parents to ensure their child's can use social networking safely.

- E-safety for Parents
- Useful links
    - CEOP
    - Thinkuknow
    - Childnet
    - Get safe on line
- Useful Docs:
    - Learning Disabilities Autism & Internet Safe
    - Wmnet e-safety leaflet
    - Brighter sparks guide
    - Orange guide for Parent
    - Parents Fact Sheet

Students- includes tips for students to ensure their own safety on social networking sites and what to do if they feel threatened or upset by anyone using technology.

- E-safety
- Face book app
- Thinkuknow?

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 who is the victim of cyber bullying. Mobile operators cannot bar a particular number from contacting a phone but some handsets do have this capacity. Action can only be taken against the perpetrators phone account with police involvement.

Contacts

O2 : ncb@o2.com Or 0870521400

Vodafone: 191 from a Vodafone phone or 08700700191 for Pay as you Go or 150 or 08700776655 for Pay as you Go

3: Call 333 from a 3 phone or 08707330333

EE:
Former Orange call 450 on an orange phone or 07973100450 for Pay as you Go, or 150 or 07973100150 for Pay Monthly)

Former T-Mobile call 150 on a t-mobile phone or 08454125000

Virgin:call 789 from a Virgin phone or 0845 6504500

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.beo.com/Safety.jsp.

Facebook:
Face book have now added a CEOP on-line safety app. Through this app advice, help and support can be obtained from the CEOP centre. Young people will be able to report instances of suspected grooming or inappropriate on-line sexual behaviour. To down load the app go to www,facebook.com/ClickCEOP**./**

Reports can also 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 email MySpace directly at schoolcare@myspace.com www.myspace.com/safety

Video and photo hosting sites

You Tube: 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:

MSM: 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.'

Chat Rooms, 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 to take down contents that breaks their terms of use.

Other Websites:

Think u Know (address) (can be accessed from E-safety on LG)
www.digizen.org/cyberbulling
www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying
www.childnet.com
www.ceop.gov.uk
www.getsafeonline.org
www.dct.gov.uk/ukccis
www.saferinternet.org.uk/helpline
www.wmnet.org.uk
www.teachers.org.uk
www.360safe.org.uk
www.saferinternet.org.uk/helpline

Shropshire Council Intranet *

(*Shropshire Council school staff that do not have access to the Council's intranet site can access information via the Schools HR team)

- Social Media information
- Employee Handbook
- Computer Facilities
- Mobile Phones

Other Sources of Assistance

Safe to Learn Cyber bullying Guidance (government publication)
Information Commissioner's Office
ACAS Workplaces and Social Networking: 'Social networking and ..How to develop a policy' and 'The Implications for Employment Relations 'pdf

2.8 Review of policy

Due to the ever changing nature of information and communication technologies it is best practice that this policy be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

ANNEX1

E-Safety

Summary of Roles & Responsibilities

The Governing Body will ensure that:

- The schools recognises its legal responsibility to protect staff from unlawful harassment as well as mental and physical injury at work.
- This schools E- Safety Policy (and related polices and practice such as staff induction) will be reviewed and monitored periodically so that staff, pupils and parents feel confident that their school effectively supports e-safety.

The Head teacher will ensure that:

- The whole school community including staff, pupils and parents are signposted to information, policies and practice about e-safety.
- That staff are provided with information and professional development opportunities with regards to understanding, preventing and responding to cyber bullying.
- Where it is not the line manager or Head teacher, ensure that the school has a nominated person as an e-safety lead to oversee, manage the recording, investigation and resolution of cyber bullying incidents.
- staff are clear who they report any breaches of e-safety to:

The nominated person as the E-safety lead will ensure that:

- Staff receive appropriate support to deal with and or respond to claims of cyber bullying.or any other breaches of e-safety.
- Incidents are dealt with in a timely manner.
- Where appropriate and in agreement of the wishes of the person who has reported the incident, report the actions to the police.
- The Local Authority is contacted as appropriate.

Staff should ensure that :

- They familiarise themselves with this e-safety policy and related procedures
- They understand and adhere to the schools E-Safety Code of Conduct-
- They never personally engage with cyber bullying incidents.
- They use social networking sites in an appropriate manner including editing or deleting any historical materials.

- They immediately report any incidents that they become aware about whether they be past or current to the nominated person appropriately and seek support

- They keep any records of the abuse including text, e-mails, voice mails, website or instant message.

- Screen print messages are made or web pages and times, dates and addressed of the site are noted.