**TheSchoolBus Compliance Manager**

Change the way you manage policies forever

TheSchoolBus Compliance Manager is a cloud-based document management solution enabling schools, academies and MATs to safely store and easily manage important policies and documents.



Cyber Bullying Policy

Last updated: 23 August 2016

Contents

[Statement of intent](#_Statement_of_Intent)

1. [Context](#_Context)
2. [Legal issues](#_Legal_Issues)
3. [Responsibilities for the prevention of cyber bullying](#_Prevention_of_Cyber)
4. [Required actions if cyber bullying occurs](#_Actions_in_the)
5. [Required actions if malicious posts or threats are made against students or teachers](#_Actions_in_the_1)
6. [Reporting](#_Reporting)
7. [Responding to cyber bullying](#_Responding_to_cyber)
8. [Support for the person being bullied](#_Support_for_the)
9. [Investigation and legal powers](#_Investigation)
10. [Working with the perpetrator](#_Working_with_the)
11. [Cyber bullying education](#_Cyber_bullying_Education)
12. [Monitoring and review](#_Monitoring_and_review)

# Statement of intent

Tor School believes that everyone in the school community has the right to learn and to teach in a healthy and caring environment, without fear of being bullied.

ICT plays an increasingly large and important part in the school curriculum.

We understand that in the wider community, pupils can, and do, access all types of material online and use technology for social networking. It is therefore important to acknowledge that sometimes, these technologies are used for unpleasant purposes. We accept that there are unfortunate misuses of this technology and we aim to address any breaches of this nature.

We recognise the existence of cyber bullying and the severity of the issue.

We are committed to:

* Educating pupils, staff and parents about cyber bullying and its consequences.
* Providing a productive and safe learning environment.
* Providing a robust policy to prevent and, if necessary, deal with cyber bullying, should it arise in school or within the school community.
* Developing and improving the policies and procedures around cyber bullying through regular evaluation and review.
* Providing a strong anti-bullying policy and acting upon it where bullying arises.

Signed by:

Headteacher Date:

Chair of Governors Date:

# Legal framework

* 1. The policy has due regard to the following legislation, including, but not limited to:
* The Communications Act 2003
* The Protection from Harassment Act 1997
  1. The policy has due regard to the following guidance, including, but not limited to:
* DfE (2016), ‘Keeping children safe in education
* DfE (2017) ‘Preventing and tackling bullying’

# Context

* 1. Bullying is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against. It is intended to hurt the recipient emotionally and/or physically. It can manifest verbally, in writing or images, and can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form especially within schools.
  2. Cyber bullying is the use of ICT, commonly a mobile phone or the internet, to deliberately upset someone else.
  3. It can be used to carry out all the different types of bullying; an extension of face-to-face bullying.
  4. It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation, and unauthorised publication of private information or images. It can include messages intended as jokes, but which have a harmful or upsetting effect.
  5. Cyber bullying may take place inside school, within the wider community, at home or travelling.
  6. It can draw bystanders into being accessories.
  7. It includes:
* Threats and intimidation
* Harassment or ‘cyber stalking’
* Vilification/defamation
* Exclusion or peer rejection
* Impersonation
* Unauthorised publication of private information or images
* Manipulation
  1. Cyber bullying may be carried out in many ways including the following:
* Threatening, intimidating or upsetting text messages
* Threatening or embarrassing pictures and video clips via mobile phone cameras
* Silent or abusive phone calls or using the victim’s phone to harass others, to make them think the victim is responsible
* Threatening or bullying emails, possibly sent using a pseudonym or someone else’s name
* Intimidating or hurtful responses to someone in a chat-room
* Unpleasant messages sent during instant messaging
* Unpleasant or untrue information posted to blogs, personal websites and social networking sites (e.g. Facebook)

# Legal issues

* 1. Cyber-bullying is generally criminal in character.
  2. It is unlawful to disseminate defamatory information in any media, including internet sites.
  3. The legislation that covers cyber bullying is section 127 of the Communications Act 2003, which makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive, or one of an indecent, obscene or menacing character.
  4. In addition, the Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.
  5. At Tor School, cyber bullying is considered as serious as any other form of bullying. Cyber bullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue, and the age of the pupil.

# Responsibilities for the prevention of cyber bullying

* 1. The headteacher is in charge of the practices and procedures outlined in this policy and will ensure that their effectiveness is monitored.
  2. The headteacher will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing cyber bullying.
  3. All members of staff will be trained to identify signs of cyber bullying and will be helped to stay informed about the technologies that children commonly use, by self-study and regular updates.
  4. A cyber safety code will be developed, and periodically reviewed and communicated to help pupils protect themselves from being caught up in cyber bullying, and to advise them on reporting any incidents.
  5. Pupils will be informed about cyber bullying through curricular and pastoral activities.
  6. Pupils and staff are expected to comply with the Acceptable Use Agreement: Secondary Schools.
  7. Parents will be provided with information and advice on cyber bullying.
  8. It is made clear in staff meetings and the staff handbook that members of staff should not have contact with current pupils on social networking sites (specifically should not be-friend pupils on Facebook). In addition, it is advisable not to have past pupils as friends.
  9. The delivery of PSHE is important and will discuss keeping personal information safe and the appropriate use of the internet. In addition, pupils will be educated about e-safety through projects in other subjects.
  10. Outside the curriculum, pupils will receive regular pastoral sessions about e-safety and cyber bullying through assemblies, conferences and Anti-Bullying Week.
  11. Pupils will have a voice through the school student council to ensure they are fully engaged and involved in evaluating and improving policy and procedures.
  12. Pupils from Year 7 will sign the Acceptable Use Agreement: Secondary Schools before they are allowed to use school computer equipment and the internet in school. Parents will be asked to confirm that they have discussed its contents with their children.
  13. Parents will be provided with information and advice on e-safety and cyber bullying via literature, talks, etc.

# Required actions if cyber bullying occurs

* 1. Advise the victim not to respond to the message.
  2. Refer to relevant policies including e-safety, acceptable computer use, anti-bullying and PHSE, and apply appropriate sanctions.
  3. Advise the pupil not to delete the message/image.
  4. Secure and preserve any evidence.
  5. Inform the sender’s e-mail service provider.
  6. Inform the headteacher and SLT.
  7. Notify parents of the pupils involved.
  8. Consider delivering a parent workshop for the school community.
  9. Consider informing the police, depending on the severity or repetitious nature of the offence.
  10. Inform the LA/MAT e-safety officer.

# Required actions if malicious posts or threats are made against students or teachers

* 1. Inform the site used and request the comments be removed if the site is administered externally.
  2. Secure and preserve any evidence including URLs, screenshots and print-outs.
  3. Inform the headteacher and SLT.
  4. Inform parents.
  5. Send all the evidence to name of contact at the Child Exploitation and Online Protection (CEOP) Centre.
  6. Endeavour to trace the origin and inform police as appropriate.
  7. Inform the LA/MAT e-safety officer.

# Reporting

* 1. At Tor School, issues of cyber bullying should be reported according to the procedures in the Anti-Bullying Policy: Pupils.

# Responding to cyber bullying

* 1. Cyber bullying will generally be dealt with according to the Anti-Bullying Policy: Pupils.
  2. A cyber bullying incident might include features different to other forms of bullying, prompting a particular response. Significant differences may include:
* Impact: possibly extensive scale and scope
* Location: the anytime and anywhere nature of cyber bullying
* Anonymity: the person being bullied might not know who the perpetrator is
* Motivation: the perpetrator might not realise that his/her actions are bullying
* Evidence: the subject of the bullying will have evidence of what has happened

# Support for the person being bullied

* 1. The feelings of the victim are paramount and, as with any form of bullying, support for the individual will depend on the circumstances.
  2. Available support will include:
* Emotional support and reassurance that it was right to report the incident.
* Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff.
* Emotional support and reassurance that they haven’t done anything wrong.
* Advice on other aspects of the code to prevent re-occurrence.
* Advice on how the perpetrator might be blocked from the individual’s sites or services.
* Actions, where possible and appropriate, to have offending material removed from the host media.
* Advice to consider changing email addresses and/or mobile phone numbers.
* Discussing contacting the police in cases of suspected illegal content.

# Investigation and legal powers

* 1. Again, the nature of any investigation will depend on the circumstances. It may include:
* Review of evidence and advice to preserve it, for example, by saving or printing (e.g. phone messages, texts, emails, website pages).
* Efforts to identify the perpetrator, which may include looking at the media, systems and sites used; however, members of staff do not have the authority to search the contents of a phone.
* Identifying and questioning witnesses.
* Contact with the CEOP centre if images might be illegal or raise child protection issues.
* Requesting a pupil to reveal a message or other phone content or confiscating a phone.
* The school has a duty to protect all of its members and provide a safe, healthy environment.
* Staff may request a pupil to reveal a message or other phone content and may confiscate a phone.

# Working with the perpetrator

* 1. Work with the perpetrator, and any sanctions, will be determined on an individual basis, in accordance with the Anti-Bullying Policy: Pupils, with the intention of:
* Helping the person harmed to feel safe again and be assured that the bullying will stop.
* Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour.
* Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour.
* Demonstrating that cyber bullying, as with any other form of bullying, is unacceptable, and that the school has effective ways of dealing with it.

# Cyber bullying education

* 1. As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of the computing and PSHE curriculum.

# Monitoring and review

* 1. This policy will be reviewed on an annual basis by the headteacher, who will make any changes necessary, taking into account previous cyber bullying incidents and the effectiveness of procedures, and will communicate changes to all members of staff.
  2. All members of staff are required to familiarise themselves with this policy as part of their induction programme.