Merchant Taylors' School

ANTI CYBER-BULLYING POLICY

Policy Custodian: *Deputy Head Information Services*
Approving Governors Committee: *Full Governing Body*
Approved: *March 2018*
Next Review: *March 2019*

Bullying incorporates acts that intentionally hurt another pupil or group of pupils physically or emotionally and are repeated over time. Bullying is a very serious matter that has the capacity to cause both extreme physical and emotional hurt either of which may be the pre-cursor to potentially life-long psychological damage on the part of the victim or victims. Bullying is often motivated by prejudice against particular groups, for example, on grounds of race, religion, culture, sex, gender, homophobia, special educational needs and disability, or because a child is adopted or is a carer - it may occur directly or through cyber-technology.

Cyber bullying occurs when an individual or group uses a variety of internet strategies (eg social websites, mobile 'phones, text messages, photographs and email); to cause distress or harm others through repeated and hostile behaviour. These include, but are not restricted to: humiliation, threats and intimidation; harassment; cyber stalking; vilification/defamation; exclusion; and rejection. Merchant Taylors' School treats cyber bullying, like all bullying, very seriously; this policy serves to bring into sharper relief issues specific to cyber-bullying that already covered synoptically in the school's Acceptable Use of Devices policy (AUP), the E-safety policy, the Data Protection Policy, the School's Privacy policy and its Anti-Bullying policy; the anti-cyber bullying policy should be read in conjunction with those policies.

Aims

This policy serves to:

- Enhance awareness of cyber-bullying and how to deal with it amongst pupils, staff and parents.
- Safeguard pupils by putting procedures in place to prevent cyber bullying and deal with it should it occur.

Awareness

- All pupils, parents, and staff sign the Acceptable Use Policy before they are allowed to use school connectivity or devices and parents are encouraged to discuss its contents with their children via Friends' Forums and our weekly newsletter *Scissorum*.
- All MTS teachers and staff receive training appropriate to their responsibility to develop e-safety practices and identify and deal with cyber bullying. They can recognise non-verbal signs and indications of cyber bullying and receive regular Safeguarding update training.
- Pupils are involved in developing our response to cyber bullying via the School Council. They receive age appropriate e-safety education through lectures and talks at Key stages 3, 4 & 5 and through the PSHCE programme (reinforced in Computing) during Key Stage 3; this programme is reinforced by section assemblies, initiatives like Anti-bullying Week, E-safety days involving both pupils and parents, Safer Internet Day and through the wider curriculum. Pupils are encouraged to be ambassadors of best E-safety practice and to support each other

in matters of cyber bullying, particularly those that extend outside the confines beyond the School setting. Anti-cyber bullying resources are available on the School Intranet.

Reporting

- Through Safe at Taylors', boys are aware that they can report bullying including cyber-bullying and bullying outside school in a variety of means including talking to their tutor, Head of Section, School Nurse, the School Counsellor, the Head Master or any of his deputies, incident forms are available to the pupils in the Library Balcony and the School has a reporting email account safe@mtsn.org.uk that is monitored regularly.

Procedures

- The IT department uses secure connections, Sophos UTM filtering filtering, firewall, management, anti-spyware software, Impero network monitoring software, anti-virus software, and corporate incident reporting procedures to safeguard the pupils.
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose; this extends to our obligations with regard to the Prevent Duty Guidance issued under section 29 of the Counter-Terrorism and Security Act, 2015. Following Home Office guidance about tackling radicalisation, MTS does not allow pupils independent access to Facebook, Twitter, Youtube, Ask.FM, Tumblr, Instagram, and Private messaging services, not limited to but including Whatsapp, Kik, Sureport and Viber, all of which are considered be potential sources of terrorist and extremist material.
- Staff are made aware of the risks posed by online activity of extremist and terrorist groups. This is achieved by circulation of the Home Office briefing notes for schools such as *How Social Media is used to encourage travel to Syria and Iraq.*
- The AUP and anti-bullying policy are reviewed annually; interim changes due to the emergence of a new technology are communicated to pupils, staff and parents via email or the weekly mailshot, *Scissorum*.
- During their period of induction all pupils, staff and parents are educated on the importance of password security, internet safety and safe working practices.
- As outlined in the School's e-safety policy, pupils involved in educational activity should not be using personal Internet connective technology on the School site or beyond without permission of supervising staff and only for a specified and purpose agreed beforehand by all participating parties. Where supervising staff take video footage of pupils engaged in relevant education activities on the School site or beyond, School owned devices must be used and the footage transferred to the School network and deleted from the device at the earliest opportunity.
- Where visitors to the School require access to Internet connective technology in cases where the purpose of their visit brings them into direct contact with pupils, the School must have been notified about this requirement in advance. Where the use of Internet connective technology has the potential to be a violation of individual privacy, consent from the individual(s) or their parents if the individual is under 12 years old need to be sought prior to the activity taking place.
- Full records are kept of all cyber bullying incidents (IT Network Abuse/Cyberbullying Record Form, Appendix 1)
- All pupils, teachers, and parents are aware that they may contact the School at any time over any internet issue that concerns them.

Investigation

- Whether the issue is raised via a tutor, a phone call to a secretary or by a teacher, it is referred to the Head of School who consults with the Deputy Head (Information Services). As appropriate, either the Head of School or the Deputy Head (Information Services) then takes responsibility for the investigation, including information retention and channels to the Second Master (who is the School's Designated Safeguarding Lead, DSL), the Head Master and the Deputy Head (Information Services).
- The School's investigation will comply with the broader framework of UK law (see Appendix 2).
- Where deemed necessary, the DSL will use (or provide information on) external reporting routes: mobile phone company, internet service provider, Childline or the Child Exploitation & Online Protection Centre (CEOP). If images are concerned, the Designated Safeguarding Lead will consult to determine whether they might be illegal or raise child protection concerns. If so, s/he will inform the DSL who will contact The **Defence Cyber Protection Partnership** (**DCPP**)**,** which may then involve the Local Authority Designated Officer (LADO), the local police in cases of actual/suspected illegal content, or CEOP.
- All teachers and pupils are aware of these procedures and that in these situations the School reserves to right to search drives, confiscate mobile devices, and obtain access to online storage and accounts.
- Pupils, parents and staff should be aware of the need to preserve evidence and records of abuse (e g Saving screenshots of messages or web-pages, retention of emails, recording dates and times etc…)
- Allegations against members of staff are handled as per other allegations following guidance in Keeping Children Safe in Education.

Sanctions

- In applying sanctions, the School considers the type and impact of the bullying. It recognises that in some cases cyber bullying may be unintentional, but reserves the right to come to its own judgement about such cyber communications and their impact on the victim. The sanctions imposed are designed convey a deterrent effect (strong sanctions such as exclusion may be necessary in cases of severe and persistent bullying or cyber bullying);

Parents

- Through the use of resources on the School Intranet about the consequences of cyber-bullying and how to report on-line abuse, parents are kept up to date about the part they can play to prevent bullying, including when they find themselves as bystanders. From time to time the School holds evenings for parents on how to combat cyber bullying and how best to act in partnership with the School.

The School aims:

- To help the person harmed to feel safe again and be assured that the bullying will stop.
- To hold the perpetrator to account, bring them to a realisation of the harm caused, deter them from repeating such behaviour and provide contexts that will enable the attitude and behaviour of the bully to change.

Useful Links:

DfE: Cyberbullying: Advice for Headteachers and Senior Staff

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice

Childline

http://www.childline.org.uk/Explore/Bullying/Pages/Bullyinginfo.aspx

CEOP:

http://www.ceop.gov.uk/

Deputy Head (Information Services)
March 2018
Review Date March 2019

Appendix 1: IT Network Abuse/Cyberbullying Record Form

Date:	
Pupil(s):	
Interviews By:	
Interview Notes:	
Supporting Documentation:	
Outcome:	

Appendix 2- Legal powers and responsibilities

- Although cyber bullying is not a specific criminal offence, there are criminal laws that can apply in terms of harassment as well as threatening and menacing communications. The School will contact the police if there is evidence to suggest the law has been broken. There are a number of offences that may be committed in the course of cyber bullying, some may be covered by more than one piece of legislation and the age of the perpetrator is not necessarily relevant although the general age of criminal responsibility (10 years) applies and prosecutions are unlikely for children under 14 years old.
- Pupils are entitled to their freedom of expression and respect for their private lives but they must not infringe the rights of others. Infringement includes, among other things, libel and slander, bullying, harassment and victimisation, inciting hatred on racial, religious and homophobic grounds, breach of confidentiality and breach of copyright.
- The following legislation may have a bearing in any of the above examples: Obscene Publications Act 1959, Protection of Children Act 1978, The Contempt of Court Act 1981, the Public Order Act 1986, the Malicious Communications Act 1988, the Computer Misuse Act 1990, the Protection from Harassment Act 1997, and the Communications Act 2003. All legislation concurs that the touchstone of a malicious communication is that it cause distress.
- UK law recognises that there is no clear boundary between behaviour within a school and the external behaviour of its pupils. The School has statutory powers to investigate incidents of bullying which occur outside of school hours and may apply appropriate sanctions.
- The Education and Inspections Act 2006 (EIA 2006) outlines the power of Head teachers to regulate the conduct of pupils when they are off site and provides defence in relation to the confiscation of mobile phones and other items. Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils when they are off site or not under the control or charge of a member of staff.
- Schoolteachers have the right to confiscate mobile phones as a disciplinary penalty and have a legal defence in respect of this in the EIA, 2006. Merchant Taylors' teachers are aware that they cannot search the contents of a pupil's mobile phone without the consent of that pupil. Should a pupil or member of staff refuse to allow the contents of his/her phone to be searched, the matter may be referred to the police, who have more extensive search powers, should the School deem it sufficiently serious.
- Whilst the School is obliged to protect all its members and provide a safe, healthy environment, Leah Bradford-Smart v West Sussex County Council, 2002 establishes that, "the school does not have the charge of its pupils all the time and so cannot directly protect them from harm all the time. At a day school that charge will usually end at the school gates... the school cannot owe a general duty to its pupils, or anyone else, to police their (the pupils) activities once they have left its charge. That is principally the duty of parents and, where criminal offences are involved, the police".