Anti-Cyberbullying Policy

This policy applies to all holiday courses and events run by Millfield Enterprises, referred to in this policy as “school” or “Millfield”.

This policy is intended to provide information to pupils and holiday course participants and students, together referred to in this policy as “pupils” and their parents, carers or guardians together referred to in this policy as “parents”.

This policy should be used in conjunction with the Anti-Bullying Policy.

Introduction

The school recognises that technology plays an important and positive role in everyone’s lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip staff and pupils with the knowledge and skills to be able to use technology safely and responsibly.

What is Cyberbullying?

Cyberbullying – definition

Mr Bill Belsey, the creator of the web site: http://www.cyberbullying.org/ defined this unpleasant and particularly intrusive phenomenon in the following terms:

“Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others."

Cyberbullying can involve Social Networking Sites, emails and mobile phones used for SMS messages and as cameras. In addition;

- It can be used to carry out all the different types of bullying; an extension of face-to-face bullying

- It can also go further in that it can invade home/personal space and can involve a greater number of people

- It can take place across different age groups; pupils, school staff and other adults can be targeted

- It can draw bystanders into being accessories

- It includes: threats and intimidation; harassment or ‘cyberstalking’; vilification/defamation; exclusion or peer rejection;

- Impersonation; unauthorised publication of private information or images ('happy-slapping'); and manipulation

- It can be an illegal act

Preventing cyberbullying

Understanding and discussion

- Staff will receive training in identifying cyberbullying and understanding their responsibilities

- Pupils and parents are provided with a Pupil Safe and Acceptable ICT Usage Policy to read which contains sections on Use of Chat, Blogging and Social Networking Facilities, Online Bullying, and Staying Within the Laws among others

Policies and procedures

- Ensure regular review and update of existing policies to include cyberbullying where appropriate.

- Millfield will keep good records of all cyberbullying incidents

- Director of ICT will keep AUPs under review as technologies develop

- Millfield will publicise rules and sanctions effectively

- The IT department will use filtering, firewall, anti-spyware software, anti-virus software and secure connections to help safeguard the pupils

Making reporting easier

- Pupils may contact the Director of Holiday Courses and Events, Mark Greenow, when they are concerned about a bullying issue. They may also contact the Designated Safeguarding Lead (DSL), Jane Zohoungbogbo, or the Deputy Designated Safeguarding Lead, Tom Jones.

- Ensure staff can recognise non-verbal signs and indications of cyberbullying with safeguarding training.

- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement.

Responding to cyber bullying

Most cases of cyberbullying will be dealt with through the school's existing Anti-bullying Policy and this must remain the framework within which incidents of bullying are investigated. However, some

features of cyberbullying differ from other forms of bullying and may prompt a particular response. The key differences are:

- impact: the scale and scope of cyberbullying can be greater than other forms of bullying

- targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets

- location: the 24/7 and anywhere nature of cyberbullying

- anonymity: the person being bullied will not always know who is bullying them

- intent: some pupils may not be aware that what they are doing is bullying

- evidence: unlike other forms of bullying, the target of the bullying will have evidence of its occurrence

- it is possible that a member of staff may be a victim and these responses apply to them too

Support for the person being bullied

- Offer emotional support; reassure them that they have done the right thing in telling someone

- Advise the person not to retaliate or reply. Instead, keep the evidence and take it to their parent or a member of staff (in the case of staff they should take it to the Director of Holiday Courses and Events - Mark Greenow, the Designated Safeguarding Lead - Jane Zohoungbogbo, or the Deputy Designated Safeguarding Lead - Tom Jones. These members of staff will in turn:

  - Advise the person to consider what information they have in the public domain
  - Unless the victim sees it as a punishment, they may be advised to change e.g. mobile phone number
  - If hurtful or embarrassing content is being distributed, try to get it removed from the web. If the person who posted it is known, ensure they understand why it is wrong and ask them to remove it. Alternatively, contact the host provider and make a report to get the content taken down.

- In some cases, the person being bullied may be able to block the person bullying from their sites and services. Appendix 1 contains information on what service providers can do and how to contact them

Investigation

- The safeguarding of the child is paramount and staff should investigate in accordance with

the Safeguarding and Child Protection Policy

- Members of staff should contact the the Director of Holiday Courses and Events - Mark Greenow, the Designated Safeguarding Lead (DSL) - Jane Zohoungbogbo, or the Deputy Designated Safeguarding Lead (DDSL) - Tom Jones for the purposes of investigation

- Interviews will be held in accordance with the Anti-Bullying Policy

- Staff and pupils should be advised to preserve evidence and a record of abuse; save phone messages, record or save-and-print instant messenger conversations, print or produce a screenshot of social network pages, print, save and forward to staff where appropriate

- If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact the DSL, who may involve the LADO (Local Authority Designated Officer), the local police in cases of actual/suspected illegal content.

- Identify the bully.

- Any allegations against staff should be handled as other allegations following guidance in Keeping Children Safe in Education September 2016

- Confiscate device(s) if appropriate

Working with the bully and applying sanctions

Sanctions will be applied by the Director of Holiday Courses and Events - Mark Greenow, the Designated Safeguarding Lead - Jane Zohoungbogbo, or the Deputy Designated Safeguarding Lead - Tom Jones as appropriate.

The aim of the sanctions will be:

- to help the person harmed to feel safe again and be assured that the bullying will stop

- to hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour

- to demonstrate to the school community that cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly

- Sanctions for any breaches of the Safe and Acceptable Usage Policy or internet/mobile phone agreements will be applied

- In applying sanctions, consideration must be given to type and impact of bullying and the possibility that it was unintentional or was in retaliation

- The outcome must include helping the bully to recognise the consequence of their actions and providing support to enable the attitude and behaviour of the bully to change

- A key part of the sanction may well involve ensuring that the pupil deletes files.

MILLFIELD ENTERPRISES

Legal duties and powers

- The school has a duty to protect all its members and provide a safe, healthy environment

- School staff may request a pupil to reveal a message or other phone content and may confiscate a phone.

- If they consider that a mobile phone may contain evidence of bullying or a crime or the potential of a crime they may investigate the specific contents relating to that act.

- Some cyberbullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997.

Reviewed: January 2012 / September 2012 / August 2013 / January 2014 / July 2014 / January 2015 / January 2016 / April 2017 / September 2017
Reviewer: ASC/ SCL
Reviewed for use by Enterprises: May 2018
Reviewed by: MOG

Additional Information

General advice on protecting yourself online and dealing with Cyberbullying

To avoid the risk of being exposed to illegal content and protecting yourself online, we recommend the following precautions:

o Do not share your personal information! This includes pictures of you or your family and friends, email addresses, mobile numbers and online IDs.

o Do not arrange to meet strangers! You may have been communicating with people you think you know online, but do you really know who they are?

o Do not open email or links on social networking pages from people you do not know or when you do not recognise the email address

o Similarly, do not open attachments or pictures you receive from unknown people or email addresses

o Ensure you have an effective filter on your PC to stop unwanted content.

o If you are regularly using search engines (such as Google, Bing or Yahoo), you can set each search engine site to a strict level of filtering. This limits what a search will bring up when entering keywords. Check your options with your preferred search engine site. Once you have chosen a

search filtering level, check these settings regularly to ensure they have not been amended or switched off.

o Viewing illegal images online can carry a penalty of up to 10 years in prison in the UK.

o Curiosity is normal on the internet, but being exposed to unwanted and potentially illegal images is not acceptable.

o Child Abuse images reflect just that; abuse of children and as such, should always be reported.

o Did you know that the age of criminal responsibility starts at age 10 in England and Wales!

General advice on how to deal with Cyberbullying

Due to the anonymous nature of digital communication, anyone with a mobile phone or internet connection can be the target of cyberbullying. Our schools have clear policies on dealing with bullying and cyberbullying, please contact the schools or view our websites for a copy of these policies.

Here are some general points to help deal with Cyberbullying:

- If you feel you are being bullied by email, text or online, do talk to someone you trust.

- Never send any bullying or threatening messages.

- Keep and save any bullying email, text or images.

- If you can make a note of the time and date bullying messages or images were sent and note any details about the sender.

- Use blocking software; you can block instant messages from certain people, “unfriend” people on social networking sites or use mail filters to block email.

- Do not reply to bullying or threatening messages or emails; this could make matters worse. It also lets the bullying people know that they have found a “live” number, email address or “active” social networking contact.

- Do not give out your personal details online; if you are in a chatroom, online game or IM session watch what you say about where you live, the school you go to, your email address, your friends and family. All these things can help someone build up a picture about you.

- Do not forward abusive texts, email or images to anyone. You could be breaking the law just by forwarding them. If they are about you, keep them as evidence.

- Do not ever give out passwords!

- Remember that sending abusive or threatening messages is against the law.

- Do report instances of cyberbullying you have seen or heard about, even if not directed at you. There is no such thing as an innocent bystander, if you have seen the posts, messages or images then you could be considered as part of it if you do not report it!

When and how to contact the service provider

Mobile Phones

All UK mobile operators have nuisance call centres set up and/or procedures in place to deal with such instances. The responses may vary, but possibilities for the operator include changing the mobile number of the person being bullied so that the bully will not be able to continue to contact them without finding out their new number. It is not always possible for operators to bar particular numbers from contacting the phone of the person being bullied, although some phone handsets themselves do have this capability. Action can be taken against the bully's phone account (e.g. blocking their account), only with police involvement.

Details of how to contact the phone operators:

O2: +44 (0) 844 8090200

Vodafone: call customer services on 191 from a Vodafone phone or on any other phone call +44 (0) 3333 040 191 for Pay Monthly customers or on +44 (0) 3333 348 069 for Pay As You Go customers.

EE: call customer services on 150 from your EE phone or on +44 (0) 845 412 5000 from a landline, or email using the 'how to contact us' section of the EE website at: or http://ee.co.uk/help/contact-us

Social networking sites

It is normally possible to block/ignore particular users on social networking sites, which should mean the user can stop receiving unwanted comments. Users can do this from within the site.

Many social network providers also enable users to pre-moderate any comments left on their profile before they are visible by others. This can help a user prevent unwanted or hurtful comments appearing on their profile for all to see. The user can also set their profile to for all to see. The user can also set their profile to "Private", so that only those authorised by the user are able to access and see their profile.

It is good practice for social network providers to make reporting incidents of cyberbullying easy, and thus have clear, accessible and prominent reporting features. Many of these reporting features will be within the profiles themselves, so they are 'handy' for the user. If social networking sites do receive reports about cyberbullying, they will investigate and can remove content that is illegal or breaks their terms and conditions in other ways. They may issue conduct warnings and they can delete the accounts of those that have broken these rules. It is also good practice for social network providers to make clear to the users what the terms and conditions are for using the service, outlining what is inappropriate and unacceptable behaviour, as well as providing prominent safety

information so that users know how to use the service safely and responsibly.

Contacts for some social network providers:

- Facebook and Bebo: reports can be made by clicking on a 'Report Abuse' link located below the user's profile photo (top left hand corner of screen) on every Bebo profile. 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. Users have the option to report suspicious online activity directly to the police by clicking the 'Report Abuse' link and them clicking the 'File Police Report' button.

- MySpace: reports can be made via the 'Ask MySpace' link: https://help.myspace.com/hc/en-us/sections/200507204-Blocking-Reporting

- Twitter: To report abuse on Twitter, go to the Help Centre then follow the guidance under Safety and Security.

Instant Messenger (IM)

It is possible to block users, or change Instant Messenger IDs so the bully is not able to contact their target any more. Most providers will have information on their website about how to do this. In addition, the Instant Messenger provider 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.

It is also good practice for Instant Messenger providers to have visible and easy-to-access reporting features on their service.

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'.

- Range of products including MSN Messenger.

- Yahoo!: when in Yahoo! Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse.'

Email providers (e.g. Hotmail and Gmail)

It is possible to block particular senders and if the bullying persists and alternative is for the person being bullied to change their email addresses. The email provider will have information on their website and how to create a new account.

Contacts of some email providers:

- Yahoo! Mail: there is a 'Help' link available to users when logged in, which contains a reporting form.

Video-hosting sites

It is possible to get content taken down from video-hosting sites, though the content will need to be illegal or have broken the terms of service of the site in other ways. On YouTube, perhaps the most

well known of such sites, it is possible to report content to the site provider an inappropriate. In order to do this, you will need to create an account (this is free) and log in, and then you will have the option to 'flag content as inappropriate'. The option to flag the content is under the video content itself.

- YouTube provides information on what is considered inappropriate at: http://www.youtube.com/yt/policyandsafety/safety.html

Chat rooms, individual website owners/forums, message board hosts

Most chatrooms should offer the user the option of blocking or ignoring particular users. Some services may be moderated, and then moderators will warn users posting abusive comments or take down content that breaks their terms of use.

Identifying the Bully

Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated. However, it is important to be aware that this may not necessarily lead to an identifiable individual. For instance, if another person's phone or school network account has been used, locating where the information was originally sent from will not, by itself, determine who the bully is. There have been cases of people using another individuals' phone or hacking into their IM or school email account to send nasty messages.

In cases where you do not know the identity of the bully, some key questions to look at:

- Was the bullying carried out on the school system? If yes, are there logs in school to see who it was? Contact the school IT helpdesk to see if this is possible.

- Are there identifiable witnesses that can be interviewed? There may be children who have visited the offending site and left comments, for example.

- If the bullying was not carried out on the school system, was it carried out on a mobile or a particular internet service (e.g. IM or social networking site)? As discussed, the service provider, when contacted, may be able to take some steps to stop the abuse by blocking the aggressor or

removing content it considers defamatory or breaks their terms of service.
However, the police will need to be involved to enable them to look into the data of another user.

- If the bullying was via mobile phone, has the bully withheld their number? If so, it is important to record the date and time of the message and contact the mobile operator. Steps can be taken to trace the call, but the mobile operator can only disclose this information to the police, so police would need to be involved. If the number is not withheld, it may be possible for the school to identify the caller. For example, another student may be able to identify the number. Content shared through a local wireless connection on mobile phones does not pass through the service providers' network and is much harder to trace. Similarly text messages sent from a website to a phone also provide difficulties for tracing for the internet service or mobile operator.

- Has a potential criminal offence been committed? If so, the police may have a duty to investigate. Police can issue a RIPA (Regulation of Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message. This may help identify the bully. Relevant criminal offences here include harassment and stalking, threats of harm or violence to a person or property, any evidence of sexual exploitation (for example grooming or inappropriate sexual contact of behaviour). A new national agency called the Child Exploitation and Online Protection Centre (CEOP) was set up in 2006 to deal with child sexual exploitation, and it is possible to report directly to them online at http://ceop.police.uk However, it is important to note that it is the sexual exploitation of children and young people, not cyberbullying, which forms the remit of CEOP.

Information about cyberbullying and civil and criminal laws

It is very important for schools to take cyberbullying seriously. It can be a very serious matter and can constitute a criminal offence. Although bullying or cyberbullying is not a specific offence in UK law, there are criminal laws that can apply in terms of harassment, for example, or threatening behaviour, or indeed – particularly for cyberbullying – threatening and menacing communications.

Some Useful Agencies/Resources

Websites and resources that offer support guidance and strategies for children, young people, schools and parents/carers to prevent all forms of bullying:

Anti-Bullying Alliance

This site offers information advice and resources on anti-bullying. It is intended to be a one stop shop where teachers can download assembly materials, lesson ideas and information including those for Anti-Bullying Week.

The site brings information, advice and resources together from more than 65 of its members, which include charities Childline, Kidscape, Mencap and the Association of Teachers & Lecturers (ATL). It

has a site called Hometown for children and young people about dealing with all forms of bullying:
http://anti-bullyingalliance.org.uk

Anti Bullying Network

An excellent Scottish Anti-Bullying site based at the University of Edinburgh dedicated to promoting a positive school ethos. It has advice for pupils, teachers, parents, on all aspects of bullying, including homophobic, racist and cyber and good case examples of schools in the region that have tried out various strategies to reduce bullying, organised under specific headings. Schools may find these useful for ideas and to adapt.
www.antibullying.net

AboutKidsHealth

A Canadian resource and website being developed at The Hospital for Sick Children, one of the largest paediatric teaching hospitals in the world. It has excellent resources on a number of topics related to children and young people's emotional health, wellbeing and safety, including behaviour, bullying and a good section on cyberbullying.
www.aboutkidshealth.ca

British Youth Council

The BYC brings young people together to agree on issues of common and encourage them to bring about change through taking collective action.
www.byc.org.uk

BBC Bullying

This provides links and resources explaining how to stop bullying.
www.bbc.co.uk/schools/parents/cyber_bullying

CEOP: (Child exploitation online protection)

A newly formed government agency that is dedicated to promoting online safety for children who may be vulnerable to sexual exploitation in chat rooms. It works with a number of charities and police across the UK and has a website for secondary age pupils called 'thinkuknow'.
www.ceop.gov.uk

ChildLine

This provides a 24 hour helpline for children and young people being bullied in the UK. Children and young people can call +44 (0) 800 1111 to talk about any problem. It is a major charity that is now housed with NSPCC. It provides training in peer support for pupils and schools and has a range of

publications and downloadable resources for children, parents and teachers.
www.childline.org.uk

Childnet International

This is a charity that aims to make the internet a safer place for children and is dedicated to internet safety. It is concerned to prevent abuse on the internet and cyber bullying. It has advice for children and parents and has some useful resources for teachers of ICT at key Stage 3 on internet safety. It is located in South London (Brockley).
www.childnet-int.org

Children's Legal Centre

This has produced a very helpful document called 'Bullying-a Guide to the Law' which can be downloaded. This publication is an essential tool for parents whose children are being bullied and for professionals providing advice in this area. It advises on actions schools are required to take to prevent and deal with bullying effectively, as well as providing practical advice on what parents can do if a school fails to support their child.
www.childrenslegalcentre.com

Equality and Human Rights Commission

This has examples of anti-harassment policies and links for education establishments to websites that provide relevant information on racist aspects of bullying.

www.equalityhumanrights.com

Kidscape

Kidscape is committed to keeping children safe from abuse. It is the first charity in the UK established specifically to prevent bullying and child sexual abuse it provides information, good resources and training for children and young people under the age of 16, their parents/carers. It offers a range of courses for professionals. It also provides courses in assertiveness training, ZAP, for children and young people and develops their confidence and skills to resist bullying and forms of abuse.
www.kidscape.org.uk

NSPCC

The NSPCC works tirelessly and promotes public campaigns to stop cruelty to children. There is advice on a number of issues related to bullying, child protection, and abuse. Kids Zone which contains details for their child protection helpline for young people who have problems at home or

are being bullied.
www.nspcc.org.uk

References:
Keeping Children Safe in Education - September 2016
Preventing and Tackling Bullying - October 2014