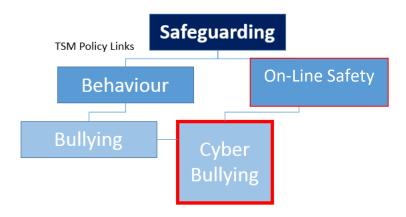


TRIMLEYST. MARTIN

Cyber Bullying Policy



Trimley St Martin Primary School

Updated March 2023

TSM Cyber Bullying Policy

Trimley St Martin Primary School believes that everyone in the school community has the right to learn and to teach in a supportive and caring environment without fear of being bullied. We are committed to helping all members of the school community to benefit from information and communication technology, whilst understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly.

Aims

This policy aims to ensure that:

- Pupils, staff and parents know about cyber bullying and its consequences;
- We have the knowledge, policies and procedures to prevent and, if necessary, to deal with cyber bullying in school or within the school community; We monitor the effectiveness of our procedures.

What is cyber bullying?

- Cyberbullying may be defined as 'the use of electronic communication, particularly mobile phones and the
 internet, to bully a person, typically by sending messages of an intimidating or threatening nature. It can
 take many forms, but can go even further than face to face bullying by invading home and personal space
 and can target one or more people.
- It can take place across age groups and target pupils, staff and others.
- It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorized publication of private information or images.
- It can include messages intended as jokes, but which have a harmful or upsetting effect.

Cyber bullying may be carried out in many ways, including:

- Threatening, intimidating or upsetting text messages;
- 'cyber-stalking' (e.g. repeatedly sending unwanted texts or instant 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;
- Menacing or upsetting responses to someone in a chat-room;
- Unpleasant messages sent during instant messaging;
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites (e.g. Facebook)
- Sexting (e.g. sending and receiving sexually explicit messages, primarily between mobile phones)

Cyber bullying and the Law

Bullying is never acceptable and the school fully recognises its duty to protect all of its members and to provide a safe, healthy environment for everyone. Bullying and cyberbullying are not specifically criminal offences. However, there are criminal and civil laws that can be used to prosecute the perpetrators of cyberbullying including:

Education Law:

- The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to Cyberbullying. Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off the school site.
- The Act also provides a defence for staff in confiscating items such as mobile phones from pupils.

Civil and Criminal Law

• There is not a specific law which makes cyberbullying illegal but it can be considered a criminal offence under several different acts including Protection from Harassment Act (1997), Malicious Communications Act TSM Cyber Bullying Policy www.trimleystmartinprimaryschool.com Page 2

(1988), Communications Act (2003) Sexual Offences Act (2013) Obscene Publications Act (1959) Computer Misuse Act (1990) and Digital Economy Act 2017.

For example, under the Malicious Communications Act 1988, it is an offence to send a communication with the intention of causing distress or anxiety; and under section 127 of the Communications Act 2003 it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character. The Protection from Harassment Act 1997 covers threatening behaviour or harassment, including online and offline stalking. If the police have enough evidence to charge the perpetrator under any of the above legislation, and they are convicted, this can act as a powerful deterrent to others. The victim may also be awarded damages because of the harm they have suffered.

Prevention of Cyber Bullying

Understanding and information

- The Head will act, as an On-Line Safety Officer, to oversee the practices and procedures outlined in this policy and monitor their effectiveness.
- The On-Line Safety Officer will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing bullying.
- Staff will be trained to identify signs of cyber bullying and will be helped to keep informed about the technologies that children commonly use.
- A Code of Advice (see Appendix 1) will be developed, periodically reviewed and communicated to help pupils protect themselves from being caught up in cyberbullying and to advise them on reporting any incidents.
- Pupils will be informed about cyber bullying through curricular and pastoral activities.
- Pupils and staff are expected to comply with the school's Use of Digital Technology Agreement Policy.
- Parents will be provided with information and advice on cyber bullying. ensure that all incidents of cyberbullying both inside and outside school are dealt with immediately

Practices and Procedures

- ✓ The responsibilities of the school and of pupils as set out in the Anti-Bullying Policy, Behaviour Policy and Child Protection & Safeguarding Policy apply also to this policy.
- ✓ Positive use of ICT will be promoted and the Use of Digital Technology Agreement Policy will be kept under review as technologies develop.
- ✓ CPD and INSET may be used to help staff develop their own practices and support pupils in safe and responsible use of ICT.
- ✓ Ensure that all staff are aware of the Prevent Duties and provide training (using Channel online awareness training module) so that staff feel confident to identify children at risk of being drawn into terrorism, to challenge extremist ideas and to know how to make a referral when a child is at risk.
- ✓ The school will encourage safe use of ICT, emphasising, for example, the importance of password security and the need to log out of accounts.
- The school will promote the message that asking for help is the right thing to do and all members of the school community will be informed how cyber bullying can be reported.
- ✓ Confidential records will be kept of all cyber bullying incidents.

Responding to cyber bullying

Cyber bullying will generally be dealt with through the schools Anti-Bullying policy. A cyber bullying incident might include features different to other forms of bullying, prompting a particular response. Key differences might be:

- ✓ 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 happened

Support for the person being bullied

As with any form of bullying, support for the individual will depend on the circumstances. Examples 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
- 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
- Advice to consider changing email addresses and/or mobile phone numbers
- Discuss contacting the police in cases of suspected illegal content

Investigation

- Again, the nature of any investigation will depend on the circumstances. It may include, for example,
- 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. Witnesses may have useful information.
- Contact with the Internet Watch Foundation, the police or the Suffolk Safeguarding Children Board Officer 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. Staff do not have the authority to search the contents of a phone.

Working with the perpetrator

Work with the perpetrator and any sanctions will be determined on an individual basis, in accordance with the Anti-Bullying Policy, 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 any other form of bullying, is unacceptable and that the school has effective ways of dealing with it.

Evaluating the effectiveness of Anti- bullying procedures

- Members of staff will report any incidents of cyber bullying to the Head teacher.
- The Head teacher will review any serious incident within three months of the school dealing with any reported cases and will ensure that an annual review of Cyber Bullying and the Anti-Bullying procedures are carried out.
- The review will take into account comments and suggested areas for improvement from staff and students, including input from the School Council.

Appendix 1

Cyber Safety Code

Guidance for Staff

The school will deal with inappropriate use of technology in line with the Code of Conduct which could result in disciplinary procedures. If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone
- · Note clearly everything on the screen relating to an inappropriate text message or image, to include the
- date, time and names
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image
- Inform the Head and Designated Safeguarding Lead immediately and pass them the information that you have

Computers

- Ask the pupil to get up on-screen the material in question
- Ask the pupil to save the material
- Print off the offending material straight away
- Make sure you have got all pages in the right order and that there are no omissions
- Inform a member of the Senior Leadership team and pass them the information that you have
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Use of Technology in School

- All members of the school community are expected to take responsibility for using technology positively.
- All staff are expected to sign to confirm they have read and understood the Acceptable Use Policy.
- All staff are expected to sign to confirm they have read and understood the Staff Behaviour Policy
- All staff are expected to have read and understood Guidelines for Staff when Children are using Digital Devices
- All children are expected to have been taken through and understood Children's Use of Digital Technology Agreement Policy

Guidance for Parents/Carers

It is vital that parents/carers and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. Parents/carers must play their role and take responsibility for monitoring their child's online life.

- Parents/carers can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.
- Parents/carers should also explain to their children legal issues relating to cyber-bullying.
- If parents/carers believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving the offensive text on their computer or on their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents/carers should contact the school as soon as possible.
- If the incident falls in the holidays the school reserves the right to take action against bullying perpetrated outside the school both in and out of term time.
- The school will ensure parents/carers are informed of the cyber-bullying policy and the procedures in place in the Anti-Bullying Policy to deal with all forms of bullying including cyber-bullying.

On-Line Safety at Home

Several sites offer helpful advice to parents/carers, particularly with respect to how they can best monitor their child's use of the computer at home. Here are some parents/carers might like to try:

www.thinkyou.know.co.uk/parents

www.saferinternet.org.uk

www.childnet.com

www.anti-bullyingalliance.org.uk

www.nspcc.org.uk

www.digizen.org

Guidance for Children

Three Steps to Safety

- 1. Respect other people online and off. Don't spread rumors about people or share their secrets, including phone numbers or passwords.
- 2. If someone insults you online or by phone, stay calm. Ignore them, but tell someone you trust.
- 3. "Do as you would be done by!" Think how you would feel if you were bullied. You are responsible for your behaviour so don't distress other people or encourage others to do so.

If you are being bullied

It is never your fault. It can be stopped and it can usually be traced.

- Don't ignore the bullying. Don't reply, but do tell someone you can trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you seem frightened or angry it will only make the person bullying you more likely to continue.

Text / video messaging

You can turn off incoming messages for a couple of days.

If bullying persists you can change your number (ask your mobile phone provider).

Do not reply to abusive or worrying messages. You can report them to you mobile phone provider.

Email

- Never reply to unpleasant or unwanted messages.
- Don't accept emails or open files from people you don't know.
- Don't delete bullying emails print them or save them as evidence in a separate folder.

Social networking sites, chat rooms and instant messaging

- Change privacy settings so you can choose who to be friends with and who can see your profile. Don't add anyone you don't know to your friend list.
- Don't use your real name in chat rooms.
- Never give out your photo or personal details, like your address, phone number or which school you go to.
- Don't post any pictures or videos you wouldn't be happy for your parents or teachers to see. Once they are
 online they can be copied and posted in other places where you can't get rid of them.
- Keep your passwords private and don't tell anyone, not even your best friend.
- To report suspicious behaviour online and to learn more about keeping yourself safe online visit www.thinkyouknow.co.uk

Always report bullying incidents. Not doing that allows the bully to continue. That's not good for the victims, for those who witness the incidents or for the bully, who may need help to change their antisocial behaviour.