



St Nicholas Church of England Primary School

'OUR CHRISTIAN COMMUNITY GROWING AND LEARNING TOGETHER'

| | |
|--------------------|------------------------------|
| Policy Title: | Cyberbullying |
| LT Responsibility: | Head Teacher |
| Review Body: | Head Teacher and Deputy Head |
| Date: | March 2021 |
| Review: | March 2023 |

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [What is cyberbullying?](#)
4. [Legal issues](#)
5. [Preventing cyberbullying](#)
6. [Signs of being cyberbullied](#)
7. [Procedures for dealing with cyberbullying](#)
8. [Support for the pupil being bullied](#)
9. [Investigation and legal powers](#)
10. [Working with the perpetrator](#)
11. [Monitoring and review](#)

Statement of intent

St Nicholas CE Primary School understands that everyone in the school community deserves to learn and teach in a supportive and caring environment, without fear of bullying or harassment.

Communication technology plays an increasingly large and important role in the school curriculum. As a result, it is important to acknowledge that, sometimes, new technologies can be used for unpleasant or illegal purposes.

We recognise the existence of cyberbullying and the severity of the issue.

The school is committed to:

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

1. Legal framework

1.1. This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The Equality Act 2010
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Regulation of Investigatory Powers Act 2000
- **[Independent schools]** The Education (Independent School Standards) Regulations 2014
- The Education Act 2002
- The Criminal Justice and Courts Act 2015
- DfE (2017) 'Preventing and tackling bullying'
- DfE (2019) 'Keeping children safe in education'
- DfE (2018) 'Searching, screening and confiscation'

1.2. This policy operates in conjunction with the following school policies:

- **Acceptable Use Agreement**
- **E-safety Policy**
- **Anti-bullying Policy: Pupils**
- **Allegations of Abuse Against Staff Policy**
- **Child Protection and Safeguarding Policy**

2. Roles and responsibilities

2.1. The Trust is responsible for:

- The overall implementation and monitoring of this policy.
- Appointing a safeguarding link governor who will work with the **DSL** to ensure the policies and practices relating to safeguarding, including the prevention of cyberbullying, are being implemented effectively.

2.2. The **headteacher** is responsible for:

- The practices and procedures outlined in this policy and ensuring that their effectiveness is monitored.
- Ensuring that the school maintains details of agencies and resources that may assist in preventing and addressing cyberbullying.
- Reviewing the procedures outlined in the school's **E-safety Policy** to ensure that pupils protect themselves from cyberbullying online.
- Ensuring all incidents of cyberbullying are reported and dealt with in accordance with the school's **Anti-bullying Policy: Pupils**.

2.3. The **DSL** is responsible for:

- Ensuring all policies that relate to safeguarding, including cyberbullying, are reviewed and updated regularly.
- Ensuring all staff are aware that they must report any issues concerning cyberbullying and know how to do so.
- Providing training to all staff so that they feel confident identifying pupils at risk of being cyberbullied and know how to make referrals when a pupil is at risk.
- Ensuring that parents are provided access to this policy so that they are fully aware of the school's responsibility to safeguard pupils and their welfare.
- Ensuring all pupils are taught about cyberbullying and how they should report a concern.
- Ensuring all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology, both inside and outside of school.

2.4. All members of staff are responsible for identifying signs of cyberbullying and staying informed about the technologies that pupils commonly use.

2.5. **Teachers** are responsible for ensuring that issues surrounding cyberbullying are explored in the curriculum and pupils are aware of how to respect others.

2.6. Pupils, staff and parents are responsible for complying with the school's **Acceptable Use Agreement**. Pupils will be asked to sign the agreement before they are allowed to use computer equipment and the internet in school. Parents will be asked to confirm that they have discussed its contents with their children.

3. What is cyberbullying?

- 3.1. For the purpose of this policy, “**bullying**” is an act which is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against and 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.
- 3.2. For the purpose of this policy, “**cyberbullying**” includes sending or posting harmful or upsetting text, images or other messages using the internet, mobile phones or other ICT for the purpose of bullying.
- 3.3. Cyberbullying can take many forms and can go even further than face-to-face bullying by invading personal space and home life, and can target more than one person. It can also take place across age groups and target pupils, staff and others, and may take place inside school, within the wider community, at home or when travelling. It can sometimes draw bystanders into being accessories.
- 3.4. Cyberbullying can include the following:
 - Threatening, intimidating or upsetting text messages
 - Threatening or embarrassing pictures and video clips sent via mobile phone cameras
 - Disclosure of private sexual photographs or videos with the intent to cause distress
 - 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 chatroom
 - Unpleasant messages sent via instant messaging
 - Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

NB. The above list is not exhaustive, and cyberbullying may take other forms.

- 3.5. All cases of cyberbullying are considered to be as serious as any other form of bullying.
- 3.6. Cyberbullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue, in accordance with the school’s **Anti-bullying Policy: Pupils.**

4. Legal issues

- 4.1. Cyberbullying is generally criminal in character.
- 4.2. It is unlawful to disseminate defamatory information in any media, including via websites.
- 4.3. Section 127 of the Communications Act 2003 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.
- 4.4. In addition, the Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.
- 4.5. At the school, cyberbullying is considered as serious as any other form of bullying. Cyberbullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue and the age of the pupil.

5. Preventing cyberbullying

- 5.1. The school recognises that both staff and pupils may experience cyberbullying and will commit to preventing any instances that may occur by creating a learning and teaching environment which is free from harassment and bullying.
- 5.2. Staff, pupils and parents will be regularly educated about cyberbullying and the importance of staying safe online, in accordance with the school's **E-safety Policy**.
- 5.3. Teachers will discuss cyberbullying as part of the curriculum, and diversity, difference and respect for others will be promoted and celebrated through various lessons.
- 5.4. Pupils will be educated about the importance of reporting instances of cyberbullying and will be fully informed of who they should report any concerns to.
- 5.5. The school will provide opportunities to extend friendship groups, and interactive skills will be provided through participation in special events, e.g. drama productions, sporting activities, etc.
- 5.6. Staff will be regularly educated about the signs of cyberbullying in order to promote early identification and intervention.

- 5.7. A cyber safety code will be developed, and periodically reviewed and communicated, to help pupils to protect themselves from being caught up in cyberbullying, and to inform them of how they can report incidents.
- 5.8. 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, not befriending pupils on Facebook). In addition, staff are discouraged from having past pupils as friends.
- 5.9. The delivery of PSHE is important and will include discussing 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, such as computing.
- 5.10. Outside the curriculum, pupils will receive regular pastoral sessions about e-safety and cyberbullying through assemblies, conferences and Anti-Bullying Week.
- 5.11. Pupils will have a voice through the student council to ensure they are fully engaged and involved in evaluating and improving policy and procedures.

6. Signs of being cyberbullied

- 6.1. All members of staff will receive training on an **annual** basis on the signs of cyberbullying, in order to identify pupils who may be experiencing issues and intervene effectively.
- 6.2. Staff will be alert to the following signs that may indicate a pupil is being cyberbullied:
 - Becoming withdrawn or shy
 - Showing signs of depression
 - Becoming extremely moody or agitated
 - Becoming anxious or overly stressed
 - Displaying signs of aggressive behaviour
 - Avoiding use of the computer
 - Changing eating and/or sleeping habits
 - Avoiding participating in activities they once enjoyed
 - Engaging in self-harm, or threatening/attempting suicide
 - Changing their group of friends suddenly

6.3. Staff will also be alert to the following signs which may indicate that a pupil is cyberbullying others:

- Avoiding using the computer or turning off the screen when someone is near
- Appearing nervous when using the computer or mobile phone
- Acting in a secretive manner when using the computer or mobile phone
- Spending excessive amounts of time on the computer or mobile phone
- Becoming upset or angry when the computer or mobile phone is taken away

6.4. Parents will also be invited to attend **annual** training sessions in order to educate them on the signs and symptoms of cyberbullying, and will be advised to report to the **headteacher** if their child displays any of the signs outlined in 6.2 and 6.3 of this policy.

7. Procedures for dealing with cyberbullying

7.1. All issues of cyberbullying should be reported according to the procedures outlined in the **Anti-bullying Policy: Pupils**.

7.2. If staff are concerned that a pupil might be at risk of cyberbullying, they will report this to the **DSL** as soon as possible.

7.3. All pupils will be informed that they can disclose cyberbullying concerns about themselves or others to any member of staff. Staff will not promise confidentiality and will inform the **DSL** of the disclosure as soon as possible.

7.4. Responses to cyberbullying incidents, including the necessary sanctions, will be dealt with in accordance with the school's **Anti-bullying Policy: Pupils**.

7.5. A cyberbullying incident might include features different to other forms of bullying, prompting a particular response. Significant differences may include the following:

- **Impact:** possible extensive scale and scope
- **Location:** the anytime and anywhere nature of cyberbullying
- **Anonymity:** the person being bullied might not know who the perpetrator is
- **Motivation:** the perpetrator might not realise that their actions are bullying

- **Evidence:** the subject of the bullying may have evidence of what has happened
- 7.6. Any cyberbullying incidents that involve members of staff will be dealt with in accordance with the school's **Anti-bullying and Harassment Policy: Staff and Allegations Against Staff Policy**.
 - 7.7. Staff are required to report any concerns to the **headteacher**, who will investigate the matter and will initiate an appropriate response.
 - 7.8. All incidents of cyberbullying, including any concerns, will be recorded and securely held by the **headteacher**.
 - 7.9. The **headteacher** will arrange a discussion with the victimised pupil in order to gain knowledge about the situation, and will use this to inform a discussion with the pupil who has been accused of cyberbullying.
 - 7.10. The **headteacher** will discuss the incident with any witnesses and will gain evidence of the cyberbullying incident; this may involve text messages, emails, photos, etc., provided by the victim.
 - 7.11. **[Primary schools]** The school understands that pupils at primary level, and particularly younger children, may not be aware of their actions and, as such, may not mean to intentionally cyberbully another pupil.
 - 7.12. The **headteacher** will take into account the nature of the cyberbullying incident and the way in which it has been conducted, including if it is evident that it was intentional or if the pupil's age and knowledge of cyberbullying is a contributing factor to the incident, when deciding on the appropriate sanction.
 - 7.13. If necessary, the **headteacher** may decide to involve the police in an appropriate response to the cyberbullying incident.
 - 7.14. If necessary, the **headteacher** will liaise with the **e-safety officer** when issuing an appropriate sanction, such as by removing internet access, monitoring the pupil's internet use, etc., in accordance with the **E-safety Policy**.

8. Support for the pupil being bullied

- 8.1. The **headteacher** will discuss the support available with the victim and, therefore, their feelings and requests are paramount to the support provided.
- 8.2. The support available includes:
 - Emotional support and reassurance from the **school counsellor**.

- Reassurance that it was right to report the incident and that appropriate action will be taken.
- Liaison with the pupil's parents to ensure a continuous dialogue of support.
- 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 e-safety procedures to prevent re-occurrence.
- Discussion with the pupil's parents to evaluate their online habits.
- Age-appropriate advice on how the perpetrator might be blocked online.
- Actions, where possible and appropriate, to have offending material removed.
- Discussion with the pupil's parents on whether police action is required (except in serious cases of child exploitation where the police may be contacted without discussion with parents).

8.3. The school will also use additional support, such as involvement with external agencies, where necessary, as outlined in the **Anti-bullying Policy: Pupils**.

9. Investigation and legal powers

9.1. The nature of any investigation will depend on the circumstances. It may include the following:

- Preserving evidence, for example, by saving or printing (e.g. phone messages, texts, emails and 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 unless the device has been seized in a lawful 'without consent' search and is prohibited by the school rules, or is suspected of being, or likely to be, used to commit an offence or cause personal injury or damage to property
- Identifying and questioning witnesses
- Contacting the CEOP centre if images might be illegal or raise child protection issues
- Requesting that a pupil reveals a message or other phone content or confiscating a phone

- Legal action, e.g. where private sexual videos or images of an individual under 16-years-old are disclosed with the intent to cause distress

10. Working with the perpetrator

10.1. How the school will work with the perpetrator and any sanctions given will be determined on an individual basis in accordance with the **Anti-Bullying Policy: Pupils**, with the intention of:

- Helping the victim 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 cyberbullying, as with any other form of bullying, is unacceptable, and that the school has effective ways of dealing with it.

11. Monitoring and review

11.1. This policy will be reviewed on an **annual** basis by the **headteacher**, who will make any changes necessary, taking into account previous cyberbullying incidents and the effectiveness of procedures, and will communicate changes to all members of staff.

11.2. All members of staff are required to familiarise themselves with this policy as part of their induction programme.

11.3. The next scheduled review date for this policy is **March 2023**