PINNER WOOD SCHOOL

Anti-Cyberbullying Policy

Approval Authority:	
Effective From:	September 2023
Date Ratified by GB:	
Next Review Date:	September 2025
Signed by Chair of GB:	

Anti-Cyberbullying Policy

This policy also applies to the Early Years Foundation Stage (EYFS) and before and after school activities.

Considerations

In accordance with the requirements, recommendations and guidance of the DfE we recognise that cyberbullying is a whole-school community issue to be embedded within our Anti-Bullying policies in order to provide a safe environment in which all members feel safe and supported.

Pinner Wood School acknowledges the assistance provided by guidance documents prepared by the following public bodies, charities and not-for- profit organisations:

- The Department for Education (DfE)
- The Independent Schools Inspectorate (ISI)
- The Office for Standards in Education (Ofsted)
- http://www.cyberbullying.org and to the site's Author, Mr Bill Belsey, whose definition of cyberbullying is quoted
- Bullying UK, Registered Charity No 1120 (www.bullying.co.uk)
- www.childnet-int.org

This policy has also been developed in accordance with the principles established by the Children Acts 1989 and 2004; the Education Act 2002, and in line with government publications: 'Working Together to Safeguard Children' 2018 (updated 2022), Revised Safeguarding Statutory Guidance 2 'Framework for the Assessment of Children in Need and their Families' 2000, 'What to do if you are Worried a Child is Being Abused' 2015. The guidance reflects, "Keeping Children Safe in Education" Sept 2023. Also this policy needs to be read in conjunction with the Child Protection Policy and Anti-Bullying Policy.

Mobile and internet technologies are generally used by adults, children and young people for their intended purposes i.e. to engage in positive communications and learning. Occasionally, however, the technology is misused in order to bully others.

It differs in several significant ways from other kinds of bullying: the invasion of home and personal space, the difficulty in controlling electronically circulated messages; the size of the audience, perceived anonymity; even the profile of the person doing the bullying and their target.

Definition of Bullying

Bullying may be defined as: *'Behaviour by an individual or group, repeated over time that intentionally hurts another individual or group, either physically or emotionally and is often motivated by prejudice against particular groups for example on grounds of race, religion, culture, sex, gender, homophobia, SEN and disability or because a child is adopted or is a carer. It may occur directly or through Cyber technology*'. Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies (see references).

Bullying is the intentional hurting, harming or humiliating of another person by physical (including sexual), verbal (including email, chat room and SMS messages), and emotional means (by excluding, tormenting or spreading malicious rumours). It can involve manipulating a third party to tease or torment someone. It can involve complicity that falls short of direct participation. Bullying is often hidden and subtle. It can also be overt and intimidatory.

A bullying incident should be treated as a Child Protection concern when there is a reasonable cause to believe that a child is suffering or likely to suffer significant harm.

Bullying may involve actions or comments that are racist, sexual, sexist or homophobic, which focus on religion, cultural background, disabilities or other physical attributes (such as hair colour or body shape). Bullying can happen anywhere and at any time and can involve anyone - pupils, other young people, staff and parents.

Cyberbullying definition

Mr Bill Belsey, the creator of the web site: 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, like Bebo, Facebook and Myspace, emails and mobile phones used for SMS messages and as cameras.

Identifying types of Cyber Bullying;

We must be aware of the different ways that ICT can be abused so that we can effectively investigate and respond to instances of online and mobile bullying. Technology can be misused in myriad ways, as highlighted by the following examples:

Computers, Consoles, IPad's, IPods, Android and windows, Tablets & Mobile phones

Bullies may make malicious - or silent - calls or send nasty, threatening, intimidating or harassing text messages.

Devices can be used to take and share humiliating images of children and young people (and staff).

Video clips of children and young people being harassed can be recorded on a device and sent to other devices or uploaded onto internet sites.

Instant messenger (IM)
Nasty messages or attachments can be sent by IM.

Bullies sometimes use someone else's IM account to forward rude or mean messages to the victim's list of friends.

Chatrooms and message boards
Bullying can happen through nasty or threatening anonymous messages.

Groups of people can use these to pick on an individual or deliberately ignore them.

Sometimes people pretend to be someone else in order to become a 'friend' and gain personal information that they then use against the victim e.g. for spreading secrets or blackmail.

Email
Email can be misused to send nasty or threatening messages.

Unsuitable images or video clips or viruses may be sent as an email attachment.

Bullies sometimes hack into a victim's account to forward personal emails or delete emails and personal contacts.

Webcams

Inappropriate content can be sent and received via webcam.

Victims may also be persuaded – or threatened – into acting in inappropriate ways that are captured on webcam.

Social networking sites
Bullies may use social networking sites to post nasty comments and humiliating images or videos.

Groups of people may pick on an individual by deliberately excluding them from a network or a friends list.

Bullies can also create distasteful fake profiles of their victim to upset or harass them or to get them into trouble.

Video hosting sites
Incidents of misuse include the posting of embarrassing or humiliating film of someone.

Virtual learning environments (VLEs)
These may be misused to post inappropriate messages or images.

Gaming sites, consoles and virtual worlds
Players may pick on weaker or less experienced users, repeatedly killing their characters.

They may also call the victim names and make abusive or derogatory remarks.

The equipment may be used to forward unwanted messages to other devices in the immediate vicinity via Bluetooth™ technology.

Signs of bullying

Changes in behaviour that may indicate that a pupil is being bullied include:

- Unwillingness to return to school
- Displays of excessive anxiety, becoming withdrawn or unusually quiet
- Failure to produce work, or producing unusually bad work, or work that appears to have been copied, interfered with or spoilt by others
- Books, bags and other belongings suddenly go missing or are damaged
- Change to established habits (e.g. giving up music lessons, change to accent or vocabulary)
- Diminished levels of self-confidence
- Frequent visits to the Medical Centre with symptoms such as stomach pains, headaches etc
- Unexplained cuts and bruises
- Frequent absence, erratic attendance, late arrival to class
- Choosing the company of adults

- Displaying repressed body language and poor eye contact
- Difficulty in sleeping, experiencing nightmares etc
- Talking of suicide or running away

Although there may be other causes for some of the above symptoms, a repetition of, or a combination of these possible signs of bullying should be investigated by parents and teachers.

Aims of this policy

- To ensure pupils, school staff and parents understand what cyber bullying is and how it can be prevented.
- To have in place procedures to prevent incidents of cyber bullying.
- To have in place effective procedures to deal with all reported incidents of cyber bullying.
- To work with other schools to share good practice in order to improve this policy.

We wish to work closely with the School Council and to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views. We as a school community have a commitment to promote equality.

Our Policy

Our school recognises that cyberbullying is the use of e-mail, instant messaging, chat rooms, pagers, mobile phones, or other forms of information technology to deliberately harass, threaten, or intimidate someone.

Cyberbullying includes text or images posted on personal websites or transmitted

via email or mobile phones as well as intimidating behaviour on gaming or social networking sites.

We also recognise that the majority of cases of cyberbullying or defamation occur outside of its controlled network. However to ensure that students and parents are aware of the correct actions to take, this policy includes advice for protection of the pupils, the school and staff members.

We aim to actively raise awareness, promote understanding about cyberbullying and build resilience to help protect themselves and their peers through discussion and activities through our Home/School Agreement, our Pupil Code of Conduct, within curriculum delivery and PSHE lessons, our pastoral care and Anti-Bullying policies including the 'Rules for Responsible Computer and Internet Use'.

Our policies will be updated regularly and reviewed regularly and at other times as considered necessary. The policy applies throughout the school, including Early Years and Before and After School Clubs.

Protection of Pupils

Pupils are given access to and are expected to use Information and Technology in accordance with the terms of our ICT Policy and Rules for Responsible Computer and Internet Use.

If a pupil is being harassed by any form of information technology then they should be advised to take the following actions immediately:

- Tell an adult that they trust. This can be a Teacher, parent, older sibling or grandparent – someone who can help you to do something about it. Either report any incidents to school themselves or ask an adult to do this for them

- Leave the area or stop the activity immediately

- If a pupil is being bullied through e-mail or instant messaging, block the sender's messages and never reply to harassing messages. They should keep a record and save any harassing messages, recording the time and date that they received them

- The Service Provider should be advised. Most service providers have appropriate use policies that restrict users from harassing others. They can respond to reports of cyberbullying over their networks, or help you track down the appropriate service provider to respond to.

- The matter must be reported to the police. If the bullying includes physical threats, or pornography tell the police. Most cases can be traced and it is a criminal offence to use a mobile phone or any form of communication to menace or harass

or offend another person.

Protection of Staff Members

Staff are given access to and are expected to use Information and Technology in accordance with the terms of our ICT Policy and Rules for Responsible Computer and Internet Use.

A case of cyberbullying/defamation against a staff member(s) of the school occurs if:

- A video or image of a school staff member(s) is placed on a public website without the permission of the staff member(s).
- Information about a staff member(s) including their name is placed on a public website without the permission of the staff member(s).
- Our school name or shield is published on a public website without the written permission of the Headteacher.

Disciplinary Action and Sanctions

Cases of cyberbullying or defamation of a member of staff, the school or the school shield, will be seriously dealt with by the Headteacher in accordance with the rules outlined in the policy and all other school based discipline policies. This may include legal consequences including criminal charges and electronic trails will be followed to gather evidence if so required.

Cases of cyberbullying or defamation of a pupil will be seriously dealt with by the Headteacher in accordance with the rules outlined in the policy and the following guidelines:

1. *Support the victim*
2. *Reassure the child or young person that they have done the right thing by telling someone.*
3. *Follow any existing pastoral support procedures and inform the victim's parents.*
4. *Advise the victim*
5. *Make sure the student knows not to retaliate or return any messages.*
6. *Ask them about the personal information they have in the public domain that the bully may be able access.*
7. *Help them to gather and keep relevant evidence for any investigation. This may include saving text messages and voicemail or noting down web addresses and taking screen shots of defamatory content online.*
8. *Give them advice on changing their contact details to prevent future incidents. Check they understand how to block unwanted contacts and know they should leave a chat room or end a call if they feel uncomfortable about unwanted contact.*
9. *Take mitigating action. When malicious content has been circulated, it is important to take action to contain the incident. If you know who the bully is, ask them to remove*

the content from the internet.

10. *Report the incident to the service provider e.g. the host of a social networking site and ask them to remove the content.*

11. *Use disciplinary powers to confiscate mobile phones being used by the bully and ask them to tell you whom they have passed any messages on to.*

12. *If the content is illegal, contact the police. They will help decide what evidence is needed and what to do with the material.* This may lead to legal consequences including criminal charges and electronic trails will be followed to gather evidence if so required.

13. *Investigate all incidents All bullying incidents will be properly recorded by the ICT Co-ordinator and investigated by the Headteacher in the same way as all other forms of bullying. Prompt notification via these routes will ensure that any incidents can be stopped before they become too serious or upsetting.*

Nevertheless, online and mobile bullying can be very serious – harassment, threats or menacing communications may even constitute a criminal offence. Students (and staff) are advised to keep a record of any bullying, which may be used as evidence.

Steps are taken to identify the bully. It may be necessary to look at the school's ICT systems. Identifying and interviewing possible witnesses may also be helpful. The school will need to contact the police before asking the service provider to look into the data of another user.

Work with the bully

Having identified the bully, the School will take steps to change their attitude and behaviour and ensure they have access to any support services they require.

Sanctions

When determining sanctions, things to consider are:

- *the impact on the victim*
- *whether the bully was acting anonymously*
- *the type of material and how widely it was circulated*
- *The motivation of the bully – was it done intentionally, unintentionally or in retaliation to bullying from others?*

Relevant sanctions may include removing or limiting the right of access to the internet for a period of time as well as suspension from school pending and post investigation as well as legal charges in respect of criminal behaviour.

The Headteacher reserves the right to confiscate any mobile or electronic devices which are brought into school or on school journeys in contradiction to the school's policies.

Promoting Safe Use of Technology

The following websites contain excellent online resources and information:

- Childnet International (www.childnet-int.org)
- Digizen (www.digizen.org.uk) -
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

Roles of people involved with this policy

1. Role of the Governors

The Governors have:

- Appointed a member of staff to be responsible for ICT;
- Delegated powers and responsibilities to the Headteacher to ensure all school personnel and visitors to the school are aware of and comply with this policy;
- Responsibility for ensuring funding is in place to support this policy;
- Responsibility for ensuring this policy and all policies are maintained and updated regularly;
- Responsibility for ensuring all relevant policies are made available to parents;
- Nominated a link governor to visit the school regularly, to liaise with the Headteacher and the coordinator and to report back to the Governing Body;
- Responsibility for the effective implementation, monitoring and evaluation of this policy

2. Role of the Headteacher

The Headteacher will:

- Ensure all school personnel, pupils and parents are aware of and comply with this policy;
- Work closely with the ICT coordinator to review how the school network is monitored;
- Ensure the ICT Policy outlines how the ICT suite and the Internet should be used;
- Provide support for those pupils and school personnel who may be victims of cyberbullying;
- Deal with all incidents of cyber bullying quickly and effectively;
- Work with parents in dealing with cyber bullying;
- Distribute an information leaflet to parents outlining how they should monitor their child's use of the internet;
- Inform parents of any incident of cyber bullying and how it has been dealt with;
- Monitor the number of recorded incidents in an academic year;
- Monitor the types of cyber bullying that occur in an academic year;
- Monitor how swiftly incidents of cyber bullying are dealt with;
- Discuss with the school council via Deputy head:
- Are pupils aware of this policy?
- How can cyber bullying be effectively dealt with?
- How good are school staff in dealing with incidents of cyber bullying?
- How good are school staff in identifying the symptoms of cyber bullying amongst pupils?
- Encourage any cyber bully to change their behaviour;
- Impose sanctions on any pupil who continues to cyber bully;
- Consider permanent exclusion in the most serious incidents of cyber bullying;
- Consider the use of legal powers under the Education Act 2006 that allow him/her to regulate behaviour of pupils when they are off-site;
- Provide guidance, support and training to all staff;
- Monitor the effectiveness of this policy;
- Annually report to the Governing Body on the success and development of this policy

3. Role of the Computing Coordinator

The coordinator will:

Work closely with the Headteacher to ensure that:

- The Acceptable Use Policy is up to date
- The school network is monitored — Using Avast Anti-Virus Protection & Server side network monitoring tools
- The school filtering system is working correctly and regularly checked for problems — We use Bespoke PfSense filtering
- Monitor the filtering logs for inappropriate content alerts
- Alert the Headteacher to Safe Guarding issues
- Information is provided for pupils and parents

* provide guidance and support to all staff;
* ensure cyber bullying is discussed during staff meetings and inset days;
* ensure cyberbullying is discussed with pupils through class discussions;

* invite pupils to consider the effects of cyberbullying;
* keep up to date with new developments and resources;
* Review and monitor;
* Manage personal data in line with statutory guidance;

4. Role of the Nominated Governor

The Nominated Governor will:

- Work closely with the Headteacher and the coordinator;
- Ensure this policy and other linked policies are up to date;
- Ensure that everyone connected with the school is aware of this policy;
- Report to the Governing Body every term;
- Annually report to the Governing Body on the success and development of this Policy

5. Role of School Staff

School personnel will:

- Comply with all the afore mentioned aspects of this policy;
- Be alert to the dangers of cyber bullying;
- Report all incidents of cyber bullying to a member of the Senior Leadership Team;
- Ensure that no pupil has unsupervised access to the Internet;
- Regularly remind pupils of:
- The safe use of the IT suite;
- The Acceptable Use Policy;
- The need to report any incident of cyber bullying to a member of the senior management team or ICT coordinator;
- Inform pupils of the dangers of cyber bullying through PSHE, collective worship, anti-bullying week activities etc;
- Be advised not to give their mobile phone numbers or email addresses to any pupil;
- Be advised not to accept as a 'friend' any pupil on to their FaceBook page or similar social media;
- Seek the views of pupils in monitoring and evaluating this policy;
- Report and deal with all incidents of discrimination;
- To attend regular safe guarding professional development that includes online safety;

6. Role of Pupils

Pupils will:

- Comply with all the afore mentioned aspects of this policy;
- Sign an Acceptable Use of ICT contract (once in KS2, signed by the parents in lower years);
- Be encouraged to report all incidents of cyber bullying to a member of the school Staff;
- Not bring mobile phones / tablets to school unless they have prior permission from the Headteacher;
- Listen carefully to all instructions given by the teacher;
- Ask for further help if they do not understand;
- Treat others, their work and equipment with respect;
- Support the school Code of Conduct and guidance necessary to ensure the smooth running of the school;
- Take part in questionnaires and surveys

7. Role of Parents

Parents will:

- Be made aware of this policy;
- Comply with this policy;
- Sign an Acceptable Use of ICT contract in lower years (EYFS, KS1);
- Be encouraged to discuss the Acceptable Use of ICT contract with their children;
- Report all incidents of cyber bullying involving their child to the school;
- Be encouraged not to use their mobile phone / tablet when on the school premises especially for the taking of photographs;
- Be asked to take part periodic surveys conducted by the school;
- Support the school Code of Conduct and guidance necessary to ensure smooth running of the school

8. Recording and Reporting

- All reported incidents are investigated and dealt with.
- Parents are informed of all events and what actions have been taken.
- Records will be kept of all incidents and their outcomes.

9. Dealing with Cyber Bullying Incidents

The Headteacher will:

- Deal with all incidents of cyber bullying quickly and effectively;
- Impose sanctions as outlined in the school's Behaviour policy on any pupil identified as being the bully;
- Confiscate any mobile phone if brought to school;
- Contact the police and social services if the cyber bullying is sufficiently severe; keep parents informed of the school's actions