Garswood Primary School Cyber Bullying Policy

In conjunction with 'GIST'

(In conjunction with Anti-bullying, Safeguarding and Online Safety Policy)

Statement of Aims

Garswood Primary School recognises that every child is unique and brings with them a wide range of skills and abilities. The whole school community works together to create a safe and happy environment in which its members are able to develop a moral code which encourages all to make a positive contribution to society. We aim to provide challenging experiences so that all can achieve their full potential.

Since the widescale use of technology as a tool for learning, socialising and play as a result of the Covid- 19 pandemic, online safety must continue to be recognised by schools as a key safeguarding consideration. The inclusion of online safety within all units of our computing scheme of work ensures that Online Safety is always at the forefront of our staff and pupils minds. that DSL and SLT feel confident that we can implement procedures to ensure that we are able to protect our communities online.

The online safety agenda continue to evolve and increase; it is therefore essential that Garswood evidence the recognition of online safety within our statutory safeguarding responsibilities and implement approaches which will safeguard our community online. DSL and SLT in schools will be constantly reviewing our current online safety practice and implement any changes as required from 1st September 2021.

Ethos:

We are committed to providing a caring, friendly and safe environment where children can learn in a secure atmosphere. Bullying of any kind is unacceptable at our school. If bullying does occur, all pupils should be able to tell and know that incidents will be dealt with promptly and effectively. We are a listening and a telling community – anyone who knows that bullying is happening is expected to tell the staff and know that the disclosure will be taken seriously.

The School's Positive Behaviour Policy promotes this environment by identifying the school rules and the procedures for enforcing them, encouraging self discipline good behaviour and respect for others.

Online Safety within 'Keeping Children Safe in Education'(KCSIE)

KCSIE is statutory guidance, and all schools and colleges must have regard to it when carrying out their safeguarding. The DfE use the terms "must" and "should" throughout the guidance; "must" is used when the person in question is legally required to do something and "should" when the advice set out should be followed unless there is good reason not to. This document only focuses on elements of KCSIE relevant to online safety. Designated Safeguarding Leads (DSLs) and leaders should read the entire document when evaluating their wider safeguarding practice.

Cyber-Bullying Policy

Virtual Bullying

With more and more of us using email and mobile phones, bullying does not have to happen in person. Silent phone calls or abusive texts or emails can be just as distressing as being bullied face-to-face.

What is Cyber-Bullying?

This is sending or posting harmful or cruel text or images using the Internet or other digital communication devices.

Research from the University of London identifies seven categories of Cyber-bullying:

Text message bullying involves sending unwelcome texts that are threatening or cause discomfort.
Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks.
Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
Chat room bullying involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.
Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online (i.e. MSN, Bebo, etc.).
Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

What can be done as a parent?

Don't wait for something to happen before you act. Make sure children understand how to use these technologies safely and know about the risks and consequences of misusing them.

- Make sure they know what to do if they or someone they know are being cyber-bullied.
- Encourage children to talk to you if they have any problems with cyber-bullying. If they do have a problem, contact the school, the mobile network or the Internet Service Provider (ISP) to do something about it.
- Parental control software can limit who your child sends emails to and who he or she receives them from. It can also block access to some chat rooms.
- Moderated chat rooms are supervised by trained adults. The ISP will tell you whether they provide moderated chat services.
- Make it your business to know what children are doing online and who your children's online friends are.

It is important that parents and carers ensure that their children are engaged in safe and responsible online behaviour. Some suggestions for parents to stay involved are:

- Keep the computer in a public place in the house. Periodically check on what your child is doing.
- Discuss the kinds of Internet activities your child enjoys.
- Be up front with your child that you will periodically investigate the files on the computer, the browser history files, and your child's public online activities.

- Search for your child's name online, look at his or her profiles and postings on teen community sites, review web pages or blogs.
- Tell your child that you may review his or her private communication activities if you have reason to believe you will find unsafe or irresponsible behaviour.
- Watch out for secretive behaviour as you approach the computer, such as rapidly switching screens, and for attempts to hide online behaviour, such as an empty history file.

What can be done as a child?

If you are being bullied, remember bullying is never your fault. It can be stopped and it can usually be traced.

- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.

There is plenty of online advice on how to react to cyber-bullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips:

Text/Video Messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists you can change your phone number (ask your Mobile service provider).
- Do not reply to abusive or worrying text or video messages - your Mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.

Email

- Never reply to unpleasant or unwanted emails.
- Don't accept emails or open files from people you do not know.
- Ask an adult to contact the sender's ISP by writing abuse@and then the host, e.g. abuse@hotmail.com.

Web

- If the bullying is on the school website or *Teams,* tell a teacher or parent, just as you would if the bullying was face-to-face.

Chat Room & Instant Messaging

- Never give out your name, address, phone number, school name or password online. It's a good idea to use a nickname. Do not give out photos of yourself either.
- Do not accept emails or open files from people you do not know.
- Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write - don't leave yourself open to bullying.

What school staff should look out for and possible actions:

Abuse and neglect

- All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to

face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. In all cases, if staff are unsure, they should always speak to the designated safeguarding lead (or deputy – Andrew Yearsley)

Action points:

- All staff receive information and training which addresses online safety at induction, and as part of accessing regularly updated safeguarding and child protection training and information. Online safety concerns are reported to the DSL.

Remote learning

- Where children are being asked to learn online at home the Department has provided advice to support schools and colleges do so safely. Please refer to the remote learning policy for how online safety requirements are met.

Filters and monitoring

Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, our staff and St Helens team as well as the governing bodies are doing all that we reasonably can to limit children's exposure to online risks such as cyberbullying. As part of this process, Garswood uses filters and monitoring systems such as Smoothwall and Windows Defender (for more details see online safety policy)

• KCSIE details support and guidance for schools regarding buying and procurement.
• At Garswood, we make informed decisions regarding the safety and security of the internet access and equipment available within or provided by our school.

The UK Safer internet Centre provide guidance about appropriate filtering and monitoring: UK Safer Internet Centre: appropriate filtering and monitoring. At Garswood our governing bodies, and DSL has read and considered this guidance when considering filtering and monitoring systems and any associated decisions.

Reviewing online safety

- Technology, and risks and harms related to it evolve and changes rapidly. Garswood carries out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks our children face. A free online safety self-review tool for schools is often utilised and can be found via the 360 safe website.
- UKCIS has published Online safety in schools: Questions from the governing board.
- The questions are used to gain a basic understanding of the current approach to keeping children safe online; and help Garswood as a staff to learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. It has also published an Online Safety Audit Tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.
- When reviewing online safety provision, the UKCIS external visitors guidance highlights a range of
- resources which can support educational settings to develop a whole school approach towards online safety.

Peer on peer /child on child abuse

All staff recognise that children are capable of abusing their peers (including online). All staff are clear about Garswood's policy and procedures with regard to peer on peer abuse. (see safeguarding policy)

Garswood's Child protection policy includes:

- procedures to minimise the risk of peer-on-peer abuse
- the systems in place (and they should be well promoted, easily understood and easily accessible)
- for children to confidently report abuse, knowing their concerns will be treated seriously
- how allegations of peer-on-peer abuse will be recorded, investigated and dealt with
- clear processes as to how victims, perpetrators and any other children affected by peer on peer abuse will be supported
- a recognition that even if there are no reported cases of peer-on-peer abuse, such abuse may still be taking place and is simply not being reported
- a statement which makes clear there is a zero-tolerance approach to abuse, and it should never be passed off as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children
- recognition that it is more likely that girls will be victims and boys' perpetrators, but that all peer on peer abuse is unacceptable and will be taken seriously

Forms of peer-on-peer abuse:

- bullying (including cyberbullying, prejudice-based and discriminatory bullying)
- abuse in intimate personal relationships between peers
    - physical abuse which can include hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm
    - sexual violence and sexual harassment.
    - Consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery): This is not tolerate under any circumstances at Garswood and depending on the severity this may lead to exclusion or parental notification.
    - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
    - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm
    - initiation/hazing type violence and rituals.

Action points:

- Staff are fully aware that these types of abuse can also happen both person to person or in an online form and have attended training in each. Our DSL and Family Support Worker has a system in place for how each incident should be dealt with and what consequences should occur.
- Garswood's child protection policy clearly identifies policies and procedures to follow when responding to online peer on peer abuse concerns e.g. consensual and non-consensual sharing of nudes and semi-nude images and/or videos

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- **unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded**

- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above
- Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), would refer into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Education for a Connected World:

Today's children and young people are growing up in a digital world. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.
Garswood will adopt philosophies from Education for a Connected World to describe the skills and understanding that children and young people should have the opportunity to develop at different ages and stages. Highlighting what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it safely.

ProjectEVOLVE:

Resources each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" with perspectives; research; activities; outcomes; supporting resources and professional development materials.
This vast library of content is managed by an innovative new engine, designed by the SWGfL Web team, that not only makes navigating the content intuitive but allows users to personalise the content they collate.
Project evolve can provide information, lesson plans, research summaries, stimulus questions and activities for pupils to complete. Professional development materials for staff are also available to broaden ever changing e safety knowledge. It has been designed with customisation and flexibility.
The content has been written by a team of experts here at the UK Safer Internet Centre. It's up to date; relevant and engaging and moves online life education into the third decade of the 21st century.

Using ProjectEVOLVE

The toolkit is based on UKCIS framework "Education for a Connected World" (EFACW) that covers knowledge, skills, behaviours and attitudes across eight strands of our online lives from early years right through to eighteen. These outcomes or competencies are mapped to age and progressive. The statements guide educators as to the areas they should be discussing with children as they develop their use of online technology.

On its own EFACW is a useful guide but also a challenge if you have to turn those statements into a learning opportunity. That's where ProjectEVOLVE comes in; it's the perfect way not only to navigate the framework but resources every single one of the 350 plus statements.

Advice from Thinkuknow.co.uk

- Know what your children are doing online and who they are talking to. Ask them to teach you to use any applications you have never used. Keeping the computer in a family room means that you can share your child's online experience – and that they are less likely to act inappropriately (i.e. via webcam).
- Help your children to understand that they should never give out personal details to online friends — personal information includes their messenger
- ID, email address, mobile number and any pictures of themselves, their family or friends. If your child publishes a picture or video online, anyone can change it or share it. Remind them that anyone may be looking at their images and one day a future employer could!
- If your child receives spam/junk email & texts, remind them never to believe them, reply to them or use them. It's not a good idea for your child to open files that are from people they don't know. They won't know what they contain — it could be a virus, or worse — an inappropriate image or film.
- Help your child to understand that some people lie online and therefore it's better to keep online mates online. They should never meet up with any strangers without an adult they trust.
- Always keep communication open for a child to know that it's never too late to tell someone if something makes them feel uncomfortable.
- Teach young people how to block someone online and how to report them if they feel uncomfortable.

Websites:

www.ceop.gov.uk
www.thinkuknow.co.uk
www.getnetwise.org
https://projectevolve.co.uk/about
https://www.gov.uk/government/publications/education-for-a-connected-world

Three Steps to Safety

1.Respect other people - online and off. Do not spread rumours about people or share their secrets, including phone numbers and passwords.

2. If someone insults you online or by phone, stay calm – and 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 own behaviour -make sure you don't distress other people or cause them to be bullied by someone else.

Not reporting a bullying incident allows the bully to continue with their bullying behaviour. This is not good for the bully, who needs help in order to change their antisocial behaviour, or for those who are the victims or those who witness such events.

There will be consequences for bullying behaviour. The consequences will vary according to the severity of the incident, but all incidents of bullying will be treated seriously by Garswood Primary School.

Les Moon (Computing lead) **September 2021**

Reviewed and updated Jan 23